



Serial-to-WiFi Adapter Application Programmer

Reference Guide

GS2011-S2W-APP-PRG-RG-001208

Module

GS2011M

Software Release

5.1.5

GainSpan® 802.11b/g/n Ultra-Low Power WiFi® Series Modules

Copyright Statement	<p>This GainSpan manual is owned by GainSpan or its licensors and protected by U.S. and international copyright laws, conventions, and treaties. Your right to use this manual is subject to limitations and restrictions imposed by applicable licenses and copyright laws. Unauthorized reproduction, modification, distribution, display or other use of this manual may result in criminal and civil penalties.</p> <p>GainSpan assumes no liability whatsoever, and disclaims any express or implied warranty, relating to sale and/or use of GainSpan products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. GainSpan products are not authorized for use as critical components in medical, lifesaving, or life-sustaining applications</p> <p>GainSpan may make changes to specifications and product descriptions at any time, without notice.</p>
Trademark	<p>GainSpan is a registered trademark of GainSpan Corporation. All rights reserved. Other names and brands may be claimed as the property of others.</p>
Contact Information	<p>In an effort to improve the quality of this document, please notify GainSpan Technical Assistance at 1.408.627.6500 in North America or +91 80 42526503 outside North America.</p>

Table of Contents

Chapter 1 Interface Architecture	23
1.1 Overview	23
1.2 Interfaces	23
1.2.1 Dual Interface	23
1.3 Architecture of Adapter	24
Chapter 2 Adapter Description	27
2.1 System Initialization	27
2.1.1 Network Configuration	28
2.1.2 Profile Definition	33
2.2 Command Processing Mode	35
2.2.1 Auto Connection	36
2.2.1.1 Auto Connection Operation	38
2.3 Data Handling	40
2.3.1 Bulk Data Tx and Rx	42
2.3.2 Unsolicited Data Handling	44
2.3.3 Software Flow Control	44
2.3.4 Hardware Flow Control	46
2.4 Serial Data Handling	47
2.5 Connection Management	48
2.5.1 Packet Reception	48
2.5.2 Remote Close	48
2.5.3 TCP Server Connections	49
2.6 Wireless Network Management	50
2.6.1 Scanning	50
2.6.2 Association	50
2.6.3 SSID and Passphrase	51
2.7 Response Codes	52
2.7.1 Enhanced Asynchronous Messages	55
2.7.2 Exception Messages	57
2.7.3 Boot Messages	58
Chapter 3 Commands for Command Processing Mode	59
3.1 Overview	61
3.2 Command Interface	62
3.2.1 Interface Verification	62
3.2.2 Echo	62
3.2.3 Verbose	63
3.3 Node Start Up Handling	64
3.4 UART Interface Configuration	65
3.4.1 UART Parameters	65
3.4.2 Software Flow Control	66
3.4.3 Hardware Flow Control	66
3.5 SPI Interface and Configuration	68
3.6 SPI Interface Handling	69
3.6.1 SPI Byte Stuffing Method	69
3.6.2 SPI DMA Command Response Method	70
3.6.2.1 Polling Methodology	71
3.6.2.2 Interrupt Based Methodology	76

3.6.2.3 Annexure - HI Frame Format (From Host Side)	80
3.6.2.4 Annexure - HI Frame Response (From GS2011M Side)	82
3.6.2.5 Pin Connection for SPI Interface	83
3.6.3 SDIO Interface	83
3.7 Serial-to-WiFi Configuration	84
3.8 Identification Information	86
3.9 Serial-to-WiFi Profile Configuration	87
3.9.1 Save Profile	87
3.9.2 Load Profile	88
3.9.3 Selection of Default Profile	89
3.9.4 Restore to Factory Defaults	90
3.9.5 Output Current Configuration	91
3.10 WiFi Interface Configuration	92
3.10.1 Set MAC Address	92
3.10.2 Get MAC Address	93
3.10.3 Set Regulatory Domain	94
3.10.4 Get Regulatory Domain	95
3.10.5 Set Scan Time	96
3.10.6 Get Scan Time	97
3.10.7 Scanning	98
3.10.8 Mode	100
3.10.9 Associate with or Create an Infrastructure (AP) Network	102
3.10.10 Disassociation	104
3.10.11 WPS	105
3.10.12 Status	107
3.10.13 Error Code	109
3.10.14 Get RSSI	110
3.10.15 Set Transmit Rate	110
3.10.16 Get Transmit Rate	112
3.10.17 Set Retry Count	113
3.10.18 Get Client Information	114
3.11 WiFi Security Configuration	115
3.11.1 Authentication Mode	115
3.11.2 Security Configuration	116
3.11.3 WEP Keys	117
3.11.4 WEP Key Type Configuration	118
3.11.5 WPA-PSK and WPA2-PSK Passphrase	118
3.11.6 WPA-PSK and WPA2-PSK Key Calculation	120
3.11.7 WPA-PSK and WPA2-PSK Key	121
3.11.8 EAP-Configuration	123
3.11.9 EAP	125
3.11.10 EAP Time Validation	127
3.11.11 Certificate Addition	128
3.11.12 Certificate Deletion	130
3.11.13 Certificate Validation	131
3.11.14 Radio Receiver in Active Mode	132
3.11.15 Radio Receiver in Power Save Mode	133
3.11.16 Enable/Disable Multicast Reception	135
3.11.17 Sync Loss Interval	138
3.11.18 Association Keep Alive Timer	139
3.11.19 IEEE PS Poll Listen Interval	140
3.11.20 WLAN Keep Alive Interval	143
3.12 Network Interface	144
3.12.1 DHCP Client Support for IPv4	144

3.12.2	Static Configuration of Network Parameters for IPv4	147
3.12.3	MDNS Module Initialization for IPv4	148
3.12.4	MDNS Host Name Registration	150
3.12.5	MDNS Host Name De-registration	152
3.12.6	MDNS Services Registration	154
3.12.7	MDNS Services De-Registration	156
3.12.8	MDNS Services Announce	158
3.12.9	MDNS Service Discover	159
3.12.10	MDNS Module De-Initialization	160
3.12.11	DHCP Server for IPv4	161
3.12.12	DHCP Server Configuration for IPv4	163
3.12.13	DNS Server	164
3.12.14	DNS Lookup (Client)	165
3.12.15	Static Configuration of DNS (Client)	167
3.12.16	IP Multicast Join	168
3.12.17	IP Multicast Leave	168
3.12.18	Store Network Context	169
3.12.19	Restore Network Context	170
3.12.20	ARP Cache Enable	171
3.12.21	ARP Entry Listing	172
3.12.22	ARP Entry Set	173
3.12.23	ARP Entry Delete	174
3.12.24	ARP Learning	175
3.12.25	Gratuitous ARP	176
3.13	Connection Management Configuration	177
3.13.1	Network Interface Filter	177
3.13.2	Get Network Interface Filter Configuration	179
3.13.3	TCP Clients for IPv4	180
3.13.4	UDP Clients for IPv4	183
3.13.5	TCP Servers for IPv4	184
3.13.6	UDP Servers for IPv4	187
3.13.7	Connection Status	189
3.13.8	Closing a Connection	191
3.13.9	Closing All Connections	192
3.13.10	Socket Options Configuration	192
3.13.11	SSL Connection Open	197
3.13.12	SSL Connection Close	198
3.13.13	SSL Configuration	199
3.13.14	HTTP Configuration	201
3.13.15	HTTP Client Configuration Clear	204
3.13.16	HTTP Client Connection Open	205
3.13.16.1	Open HTTP Connection Using Non-authenticated Proxy Server	207
3.13.16.2	Open HTTPS Connection Using Non-authenticated Proxy Server	208
3.13.16.3	Open HTTPS Connection Using Domain Name Verification	209
3.13.17	HTTP Client Data Exchange	211
3.13.18	HTTP Client Close	212
3.13.19	Data Transfer in Bulk Mode	212
3.13.20	Data Drop	212
3.14	Unassociated Frame Transmission and Reception	214
3.14.1	Unassociated Mode	214
3.14.2	Start Data Reception in Unassociated Mode	219
3.14.3	Stop Data Reception in Unassociated Mode	222
3.15	ISO TX	223
3.15.1	ISO TX Transmission Start	223

3.16	GSLINK	225
3.16.1	Start/Stop Webserver	225
3.16.2	Enable or Disable XML Parser on HTTP Data	227
3.16.3	Send XML/Raw HTTP Data	228
3.16.4	Receive XML\Raw HTTP Data	232
3.16.5	URI Modification	234
3.17	CoAP	235
3.17.1	CoAP Client Option Configuration	235
3.17.2	CoAP Client Option Configuration Removal	236
3.17.3	CoAP Client Connection Open	237
3.17.4	CoAP Client Connection Send	239
3.17.5	CoAP Client Connection Close	240
3.18	Using CoAP with GSLink	241
3.19	Battery Check	242
3.19.1	Battery Check Start	242
3.19.2	Battery Warning/Standy Level Set	243
3.19.3	Battery Check Set	244
3.19.4	Battery Check Stop	245
3.19.5	Battery Value Get	245
3.20	Power State Management	246
3.20.1	Enable Deep Sleep	246
3.20.2	Configure Power Save in Limited AP Mode	248
3.20.3	Request Standby Mode	250
3.21	Auto Connection	252
3.21.1	Wireless Parameters	252
3.21.2	Network Parameters	253
3.21.3	Enable Auto Connection	255
3.21.4	Initiate Auto Connect	256
3.21.5	Exit from Auto Connect Data Mode	257
3.21.6	Return to Auto Connect Mode	257
3.21.7	Use Cases for Auto Connect Mode	257
3.22	Network Connection Manager (NCM)	259
3.22.1	NCM Start/Stop	259
3.22.2	NCM Configuration	261
3.22.3	NCM Status Get	263
3.22.4	NCM AP Configuration Enable	264
3.22.5	Use Cases for NCM	266
3.23	Roaming	267
3.24	Provisioning	269
3.24.1	Web Provisioning Start	269
3.24.2	Web Provisioning Stop	274
3.24.3	HTTPD Redirection	274
3.24.4	Group Provisioning	275
3.25	RF Tests	277
3.25.1	RF Tests for GS2011M	277
3.25.1.1	RF Test Mode Start for GS2011M	277
3.25.1.2	RF Test Mode Stop for GS2011M	277
3.25.1.3	Asynchronous Frame Transmission for GS2011M	277
3.25.1.4	Asynchronous Frame Reception Start for GS2011M	280
3.25.1.5	Asynchronous Frame Reception Stop for GS2011M	282
3.25.1.6	Asynchronous Frame Transmission (TX99 mode) for GS2011M	283
3.25.1.7	Asynchronous Frame Transmission (TX100 mode) for GS2011M	289
3.25.1.8	Carrier Wave Transmission for GS2011M	291
3.26	Miscellaneous	292

3.26.1 Enhanced Asynchronous Notification	292
3.26.2 Set System Time	294
3.26.3 Set System Time Using SNTP	294
3.26.4 Get System Time	295
3.26.5 GPIO Out HIGH/LOW	295
3.26.6 Version	296
3.26.7 Ping for IPv4	298
3.26.8 Reset	299
3.26.9 WLAN Statistics for GS2000	299
3.26.10 Hardware Cryptography	302
3.27 Over the Air Firmware Upgrade Using External Flash	303
3.27.1 FWUP Configuration	303
3.27.2 FWUP Start	304
3.28 ADC Commands	306
3.28.1 ADC Configuration	306
3.28.2 ADC Start	308
3.28.3 ADC Read	308
3.28.4 ADC Stop	310
3.28.5 Use Case for ADC	310
3.29 I2C Commands	311
3.29.1 I2C Configuration	311
3.29.2 I2C Start	312
3.29.3 I2C Write	312
3.29.4 I2C Read	313
3.29.5 I2C Stop	313
3.30 Pulse Width Modulation (PWM) Commands	314
3.30.1 PWM Start	314
3.30.2 PWM Stop	317
3.30.3 PWM Control	317
Appendix A Data Handling Escape Sequences	319
A.1 UART Interface	319
A.2 SPI Interface	323
Appendix B Serial-to-WiFi Commands	327
B.1 Command Interface	328
B.2 UART/ADAPTER Interface Configuration	329
B.3 Profile Management	330
B.4 GSLINK	331
B.5 CoAP	332
B.6 WiFi Interface	333
B.7 WiFi Security	336
B.8 Wireless Configuration	338
B.9 Network Interface	339
B.10 Connection Management	342
B.11 Battery Check	345
B.12 Power Management	346
B.13 Auto Connection	347
B.14 RF Test	348
B.15 ADC Commands	349
B.16 I2C Commands	349
B.17 PWM Commands	350
B.18 Miscellaneous	351
B.19 Default Return Messages	354

B.20 Escape Sequence Commands	355
-------------------------------------	-----

About This Manual

This manual provides guidelines for using the GainSpan® AT command-line interface to design, configure, and provision the GS2011M series module in a WiFi network, using serial commands.

Refer to the following sections:

- [Revision History, page 9](#)
- [Audience, page 11](#)
- [Standards, page 11](#)
- [Documentation Conventions, page 12](#)
- [New and Changed AT Commands, page 15](#)
- [Documentation, page 17](#)
- [References, page 19](#)
- [Contacting GainSpan Technical Support, page 20](#)
- [Returning Products to GainSpan, page 21](#)
- [Accessing the GainSpan Portal, page 22](#)

Revision History

This revision history of the *GainSpan Serial-to-WiFi Adapter Application Programmer Reference Guide* is maintained in the following table:

Table 1 Revision History

Version	Date	Remarks
1.0	March 2015	Initial Release Added command AT+DROPDATAEN. See 3.13.20 Data Drop, page 212 . Added a new value for parameter <i>Configuration ID</i> to See section 3.13.13 SSL Configuration, page 199 .
2.0	April 2015	Added a new parameter 3.13.14 HTTP Configuration, page 201 . Added information about DataInterfaceReady in 1.2.1 Dual Interface, page 23 .

Table 1 Revision History (Continued)

Version	Date	Remarks
2.0	April 2015	<p>Updated ATSn with the following:</p> <ul style="list-style-type: none"> Added <i>parameter</i> 8 for Auto connection exit sequence enabled timeout. Added a note for <i>parameter</i> 7 to support infinite retries <p>See 3.7 Serial-to-WiFi Configuration, page 84.</p> <p>Updated the following under parameter <i>Reception frame type</i>:</p> <ul style="list-style-type: none"> Removed 128: Non-directed management frame Added a note under 64: Directed management frame <p>See Table 194 Unassociated Mode Data Transmission or Reception Parameters, page 214.</p> <p>Updated <i>Out of StandBy-Timer</i> under <i>Asynchronous Messages</i> in Table 14 Response Codes, page 52.</p> <p>Updated the example for AT+L2CONFIG command in 3.13.2 Get Network Interface Filter Configuration, page 179.</p> <p>Updated AT+WEBPROV command with the following changes:</p> <ul style="list-style-type: none"> Added default value for parameter <i>SSL Enabled</i>. Added <i>Mode values</i> for <i>WEP_AUTH_MODE</i> and <i>AP-WEP_AUTH_MODE</i> for parameter <i>ParamStoreOption</i>. Updated description for parameters <i>user name</i> and <i>password</i>. Updated the following provisioning information for parameter <i>ParamStoreOption</i>: <i>AP-DHCPSVR-STARTI</i>, <i>DHCPSVR-NO-CONN</i>, and <i>AP-DNSSRVR-ENABLE</i>; and added '=' for <i>NEW_USER_NAME</i>. <p>Updated parameter <i>Max scan time</i> in AT+WST command. See 3.10.5 Set Scan Time, page 96.</p> <p>Removed parameter <i>size of the certificate</i> from ESC<W> sequence in AT+TCERTADD command. See 3.11.11 Certificate Addition, page 128.</p> <p>Added DHCP Server under Prerequisites for 3.24.4 Group Provisioning, page 275.</p> <p>Removed parameters <i>Send response status line</i> and <i>Send response headers count</i> from AT+XMLSEND and AT+HTTPSEND commands. See 3.16.3 Send XML/Raw HTTP Data, page 228.</p>

Audience

This manual is designed for software engineers who want to evaluate, design, and implement *GainSpan Ultra Low Power 802.11 WiFi Modules* within their environment. To use this manual you will need a basic understanding of WiFi networks, network principles, and network protocols.

Standards

The standards that are supported by the GainSpan GS module series are:

- IEEE 802.11 b/g/n

Documentation Conventions

This manual uses the following text and syntax conventions:

- Special text fonts represent particular commands, keywords, variables, or window sessions
- Color text indicates cross-reference hyper links to supplemental information
- Command notation indicates commands, subcommands, or command elements

[Table 2, page 12](#), describes the text conventions used in this manual for software procedures that are explained using the AT command line interface.

Table 2 Document Text Conventions

Convention Type	Description
command syntax monospaced font	This monospaced font represents command strings entered on a command line and sample source code. AT XXXX
Proportional font description	Gives specific details about a parameter. <Data> DATA
UPPERCASE Variable parameter	Indicates user input. Enter a value according to the descriptions that follow. Each uppercased token expands into one or more other token.
lowercase Keyword parameter	Indicates keywords. Enter values exactly as shown in the command description.
[] Square brackets	Enclose optional parameters. Choose none; or select one or more an unlimited number of times each. Do not enter brackets as part of any command. [parm1 parm2 parm3]
?	Used with the square brackets to limit the immediately following token to one occurrence.
<ESC> Escape sequence	Each escape sequence <ESC> starts with the ASCII character 27 (0x1B). This is equivalent to the Escape key. <ESC>C
<CR> Carriage return	Each command is terminated by a carriage return.
<LF> Line feed	Each command is terminated by a line feed.
<CR><LF> Carriage return Line feed	Each response is started with a carriage return and line feed with some exceptions.

Table 2 Document Text Conventions (Continued)

Convention Type	Description
<>	Enclose a numeric range, endpoints inclusive. Do not enter angle brackets as part of any command.
Angle brackets	<SSID>
=	Separates the variable from explanatory text. Is entered as part of the command.
Equal sign	PROCESSID = <CID>
.	Allows the repetition of the element that immediately follows it multiple times. Do not enter as part of the command.
dot (period)	.AA:NN can be expanded to 1:01 1:02 1:03.
A.B.C.D	IPv4-style address.
IP address	10.0.11.123
LINE	Indicates user input of any string, including spaces. No other parameters may be entered after input for this token.
End-to-line input token	string of words
WORD	Indicates user input of any contiguous string (excluding spaces).
Single token	singlewordnospaces

Table 3, page 14, describes the symbol conventions used in this manual for notification and important instructions.

Table 3 Symbol Conventions

Icon	Type	Description
	Note	Provides helpful suggestions needed in understanding a feature or references to material not available in the manual.
	Alert	Alerts you of potential damage to a program, device, or system or the loss of data or service.
	Caution	Cautions you about a situation that could result in minor or moderate bodily injury if not avoided.
	Warning	Warns you of a potential situation that could result in death or serious bodily injury if not avoided.
	Electro-Static Discharge (ESD)	Notifies you to take proper grounding precautions before handling a product.

New and Changed AT Commands

The following AT commands are new (N) or have changed (C) in the software release.

[Table 4, page 15](#) lists and describes additions and changes to the GainSpan AT release. Minor changes, such as changes in range values, default values, or changes in command requirements from required to optional are not documented.

Table 4 New or Changed AT Commands

N	C	Command	Description
X		AT+DROPDATAEN	Added command AT+DROPDATAEN. See 3.13.20 Data Drop, page 212 .
X		AT+SSLCONF	Added a new value for parameter <i>Configuration ID</i> to See section 3.13.13 SSL Configuration, page 199 .
X		AT+HTTPCONF	Added a new parameter 3.13.14 HTTP Configuration, page 201 .
X		AT+WEBPROV	Updated AT+WEBPROV command with the following changes: <ul style="list-style-type: none">• Added default value for parameter <i>SSL Enabled</i>.• Added <i>Mode values</i> for <i>WEP_AUTH_MODE</i> and <i>AP-WEP_AUTH_MODE</i> for parameter <i>ParamStoreOption</i>.• Updated description for parameters <i>user name</i> and <i>password</i>. Updated the following provisioning information for parameter <i>ParamStoreOption</i> : <i>AP-DHCPSRVR-STARTI</i> , <i>DHCPSRVR-NO-CONN</i> , and <i>AP-DNSSRVR-ENABLE</i> ; and added '=' for <i>NEW_USER_NAME</i> .
X		AT+XMLSEND	Removed parameters <i>Send response status line</i> and <i>Send response headers count</i> from AT+XMLSEND command. See 3.16.3 Send XML/Raw HTTP Data, page 228 .
X		AT+HTTPSEND	Removed parameters <i>Send response status line</i> and <i>Send response headers count</i> from AT+HTTPSEND command. See 3.16.3 Send XML/Raw HTTP Data, page 228 .
X		AT+WST	Updated parameter <i>Max scan time</i> in AT+WST command. See 3.10.5 Set Scan Time, page 96 .
X		AT+TCERTADD	Removed parameter <i>size of the certificate</i> from <i>ESC<W></i> sequence in AT+TCERTADD command. See 3.11.11 Certificate Addition, page 128 .
			Removed parameters <i>Send response status line</i> and <i>Send response headers count</i> from AT+XMLSEND and AT+HTTPSEND commands. See 3.16.3 Send XML/Raw HTTP Data, page 228 .

Documentation

The GainSpan documentation suite listed in [Table 5, page 17](#) includes the part number, documentation name, and a description of the document. The documents are available from the GainSpan Portal. Refer to [Accessing the GainSpan Portal, page 22](#) for details.

Table 5 Documentation List

Part Number	Document Title	Description
GS2K-QS-001205	GainSpan GS2000 Based Module Kit Quick Start Guide	Provides an easy to follow guide on how to unpack and setup GainSpan GS2000 based module kit for the GS2000 based modules.
GS2K-EVB-FP-UG-001206	GainSpan GS2000 Based Module Programming User Guide	Provides users steps to program the on-board Flash on the GainSpan GS2000 based modules using DOS or Graphical User Interface utility provided by GainSpan. The user guide uses the evaluation boards as a reference example board.
GS2K-SMP-EXP-UG-001207	GainSpan GS2000 Based Module Sample Examples for using Serial-to-WiFi AT Commands to Create TCP or UDP Connection User Guide	Provides an easy to follow instructions on how to setup, create, and run connection examples for UDP client/server and TCP client/server. This manual also provides instructions for provisioning the board, setting up Limited AP mode, and WiFi Protected Setup (WPS), and Web provisioning over Ad-hoc.
GS2K-SDK-DB-UG-001209	GS2000 Based Module Software Development Kit and Debugging User Guide	This manual provides SDK user installation instructions, IAR IDE workbench application, and I-Jet hardware used for JTAG Serial-to-WiFi (S2W) and TLS application development and debugging.
GS2K-EVB-HW-UG-001210	GainSpan GS2000 Based Module Evaluation Board Hardware User Guide.	Provides instructions on how to setup and use the GS2000 based module evaluation board along with component description, jumper settings, board specifications, and pinouts.
GS2011M-DS-001211	GainSpan GS2011M Low Power WiFi Module Data Sheet	Provides information to help WiFi system designers to build systems using GainSpan GS2011M module and develop wireless applications.

Table 5 Documentation List (Continued)

Part Number	Document Title	Description
GS2K-HTTP-EAP-UG-001213	GainSpan GS2000 Based Module Configuration Examples for using Serial-to-WiFi AT Commands to Create HTTP, HTTPS, and EAP Connection User Guide	Provides an easy to follow instructions on how to setup, create, and run connection examples for HTTP, HTTPS, and EAP.
GS2011MxxS-DS-001214	GainSpan GS2011MxxS Low Power WiFi Module Data Sheet	Provides information to help WiFi system designers to build systems using GainSpan GS2011MxxS module and develop wireless applications.
GS2K-SDK-BLDR-UG-001223	GainSpan GS2000 Based Module Software Developer Kit (SDK) Builder User Guide	Allows OEMs and system developers to configure and generate custom firmware binary images for GainSpan low power embedded GS2000 based WiFi modules. The SDK Builder supports the GainSpan GEPS software released, including the corresponding WLAN firmware.
GS2K-SDK-QS-001225	GainSpan GS2000 Based Module Software Development Kit Quick Start Guide	Provides an easy to follow guide that will walk you through easy steps to setup, evaluation, develop, and debug the full capabilities and features of the GS2011M embedded platform software.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments by logging into [GainSpan Support Portal](#). If you are using e-mail, be sure to include the following information with your comments:

- Document name
- URL or page number
- Hardware release version (if applicable)
- Software release version (if applicable)

References

The GainSpan references listed in [Table 6, page 19](#) are available on the GainSpan Portal. Refer to [Accessing the GainSpan Portal](#), page 22 for details.

Table 6 Other Documents and References

Title	Description
Schematics	GS2000 Based Module Evaluation Board schematics supporting: GS2011M
Module Firmware and Programming Utilities	<ul style="list-style-type: none"> • Serial-to-WiFi (S2W) based firmware • Temperature and Light Sensor (TLS) based firmware <ul style="list-style-type: none"> – For use with GS2011M EVK only • Firmware Release Notes • GSFlashprogram utility for programming the modules
Smart Phone Applications	<ul style="list-style-type: none"> • Smart Phone applications for iOS and Android to evaluate and demonstrate the Temperature and Light Sensor (TLS) firmware. <ul style="list-style-type: none"> – For use with GS2011M EVK only
Software Utilities	Serial terminal program to evaluate and demonstrate Serial-to-WiFi (S2W) applications

Contacting GainSpan Technical Support

Use the information listed in [Table 7, page 20](#), to contact the GainSpan Technical Support.

Table 7 GainSpan Technical Support Contact Information

North America	1 (408) 627-6500 - techsupport@gainspan.com
Outside North America	Europe: EUsupport@gainspan.com China: Chinasupport@gainspan.com Asia: Asiasupport@gainspan.com
Postal Address	GainSpan Corporation 3590 North First Street Suite 300 San Jose, CA 95134 U.S.A.

For more Technical Support information or assistance, perform the following steps:

1. Point your browser to <http://www.gainspan.com>.
2. Click **Contact**, and click **Request Support**.
3. Log in using your customer **Email** and **Password**.
4. Select the **Location** and click **Contact**.
5. Select **Support Question** tab.
6. Select **Add New Question**.
7. Enter your technical support question, product information, and a brief description.

The following information is displayed:

- Telephone number contact information by region
- Links to customer profile, dashboard, and account information
- Links to product technical documentation
- Links to PDFs of support policies

Returning Products to GainSpan

If a problem cannot be resolved by GainSpan technical support, a Return Material Authorization (RMA) is issued. This number is used to track the returned material at the factory and to return repaired or new components to the customer as needed.



NOTE: *Do not return any components to GainSpan Corporation unless you have first obtained an RMA number. GainSpan reserves the right to refuse shipments that do not have an RMA. Refused shipments will be returned to the customer by collect freight.*

For more information about return and repair policies, see the customer support web page at: <https://www.gainspan.com/secure/login>.

To return a hardware component:

1. Determine the part number and serial number of the component.
2. Obtain an RMA number from Sales/Distributor Representative.
3. Provide the following information in an e-mail or during the telephone call:
 - Part number and serial number of component
 - Your name, organization name, telephone number, and fax number
 - Description of the failure
4. The support representative validates your request and issues an RMA number for return of the components.
5. Pack the component for shipment.

Guidelines for Packing Components for Shipment

To pack and ship individual components:

- When you return components, make sure they are adequately protected with packing materials and packed so that the pieces are prevented from moving around inside the carton.
- Use the original shipping materials if they are available.
- Place individual components in electrostatic bags.
- Write the RMA number on the exterior of the box to ensure proper tracking.



CAUTION! *Do not stack any of the components.*

Accessing the GainSpan Portal

To find the latest version of GainSpan documentation supporting the GainSpan product release you are interested in, you can search the GainSpan Portal website by performing the following steps:



NOTE: You must first contact GainSpan to set up an account, and obtain a customer user name and password before you can access the GainSpan Portal.

1. Go to the [GainSpan Support Portal](#) website.
2. Log in using your customer **Email** and **Password**.
3. Click the **Actions** tab to buy, evaluate, or download GainSpan products.
4. Click on the **Documents** tab to search, download, and print GainSpan product documentation.
5. Click the **Software** tab to search and download the latest software versions.
6. Click the **Account History** tab to view customer account history.
7. Click the **Legal Documents** tab to view GainSpan Non-Disclosure Agreement (NDA).
8. Click **Download** on the Item Browser section to open or save the document.

Chapter 1 Interface Architecture

This chapter describes the Serial-to-WiFi adapter interface architecture.

- [Overview, page 23](#)
- [Interfaces, page 23](#)
- [Architecture of Adapter, page 24](#)

1.1 Overview

The Serial-to-WiFi stack is used to provide WiFi capability to any device having a serial interface. This approach offloads WLAN, TCP/IP stack and network management overhead to the WiFi chip, allowing a small embedded host (for example an MCU) to communicate with other hosts on the network using a WiFi wireless link. The host processor can use serial commands to configure the Serial-to-WiFi Adapter and to create wireless and network connections.

1.2 Interfaces

The embedded host can use either one of the interfaces (UART/SPI/SDIO) to connect to the Serial-to-WiFi adapter.

1.2.1 Dual Interface



NOTE: *Dual Interface is supported with software release 5.1.0 and later.*

The Serial-to-WiFi adapter supports a feature called dual interface so that the embedded host can communicate to the adapter over two interfaces. One interface (primary) is used for AT command/responses and the other interface (secondary) is used for data transmission/receive.

The Serial-to-WiFi adapter supports the following combinations for dual interface (see [Table 8, page 23](#)).

Table 8 Serial-to-WiFi Dual Interface Combinations

Primary	Secondary
UART0	UART1
UART0	SPI
UART0	SDIO



NOTE: Primary interface is used for Command communication and Secondary interface is used for Data communication. The configuration parameters for the secondary interface should be given by the user when the Serial-to-WiFi adapter firmware image gets created.

UART interface which is the primary interface acts as a control path that issues AT commands and receives responses for the issued commands. SPI interface which is the secondary interface is used for sending and receiving data.

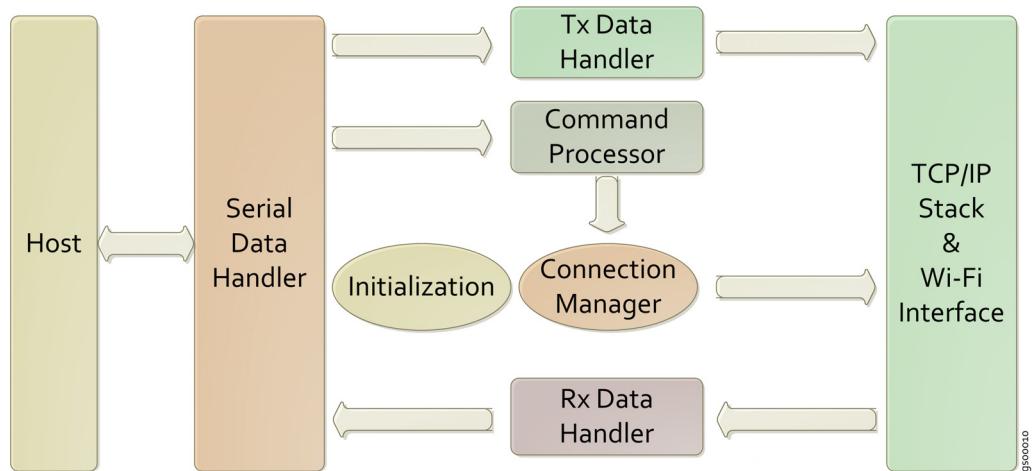
Serial-to-WiFi sends **Serial2Wifi** message on UART interface after power cycling GS module and sends **DataInterfaceReady** message on SPI interface.

UART interface does not accept any AT commands until the SPI master reads **DataInterfaceReady** message.

1.3 Architecture of Adapter

The overall architecture of the Serial-to-WiFi (S2W) interface is shown in [Figure 1, page 24](#). Transmit (Tx) and Receive (Rx) Data Handlers pass messages to and from the TCP/IP network. Commands related to management of the S2W interface and the network connections are intercepted by a Command Processor. A Serial Data Handler translates data to and from a UART/SPI/SDIO-compatible format.

Figure 1 Overall Architecture of the Adapter



The Serial-to-WiFi Adapter consists of the following modules:

- [Serial Interface Detection, page 25](#)
- [Command Processing Mode, page 35](#)
- [Data Handling, page 40](#)
- [Serial Data Handling, page 47](#)

- [Connection Management, page 48](#)
- [Wireless Network Management, page 50](#)

The software for the Serial-to-WiFi Adapter is mainly driven using a state machine. Upon powering on, the required initialization of all the modules is performed and then the state machine is entered. This state machine is event-driven and processes the events received from either the serial port or from the WiFi/Network interface as well as internal events from its own modules. The state machine calls the appropriate handler for a given event per the current state.

The Serial-to-WiFi Adapter has three distinct operating modes ([Figure 1, page 24](#)). In the default **command processing operating** mode, commands to configure and manage the interface are sent over the serial interface. In the default mode, the node accepts commands entered by the Host CPU and processes each of the commands. All commands are available in this mode. The User can establish a data connection here and send data.

In **auto connection** mode, data sent over the serial interface is transparently sent over the IP network to a single, pre-configured IP address/port pair, where data from that address is transparently sent over the UART/SPI to the serial host. With Auto mode, the IP Layer connections are already established and the data is sent directly to the target destination. In this mode, the node does not accept all commands. To accept commands the node needs to be brought back to “Command Processing” mode. Auto connection mode is entered using a serial command (see [3.21.4 Initiate Auto Connect, page 256](#)) and terminated using a special escape sequence (see [2.3 Data Handling, page 40](#)).

In **data processing** mode, data can be sent to, or received from, any of 16 possible connections. Each connection consists of a TCP or UDP path to a destination IP address and port.

For each mode, configuration parameters are stored in non-volatile memory. In addition to factory-default parameter values, two user-defined profiles (0 and 1) are available. The parameter set to be used is determined by a user command (see [3.9.3 Selection of Default Profile, page 89](#)).

- This page intentionally left blank -

Chapter 2 Adapter Description

This chapter describes the Serial-to-WiFi (S2W) operating modes.

- [System Initialization, page 27](#)
- [Command Processing Mode, page 35](#)
- [Data Handling, page 40](#)
- [Serial Data Handling, page 47](#)
- [Connection Management, page 48](#)
- [Wireless Network Management, page 50](#)

2.1 System Initialization

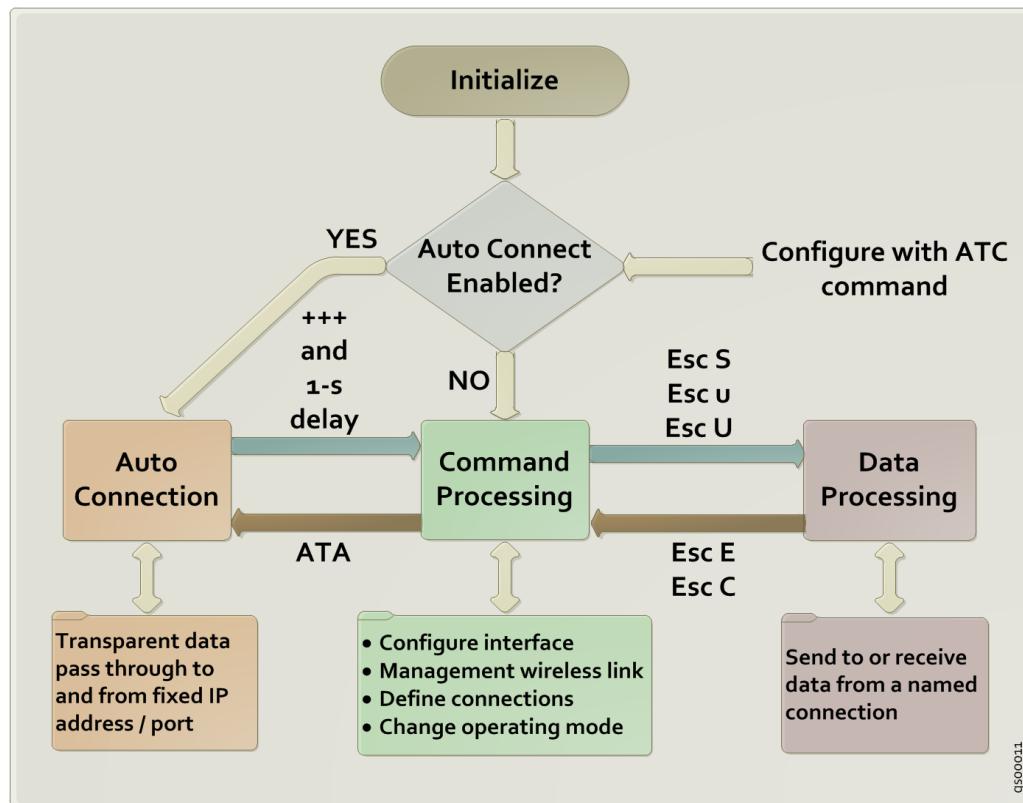
Upon startup, the Serial-to-WiFi (S2W) interface performs the following actions as displayed in [Figure 2, page 28](#).

- During the initialization process, the module will search for a saved configuration file. The configuration file include the auto connection settings, default profile and profile settings. If a saved configuration file is available, it is loaded from non-volatile memory. If no saved configuration file, the default settings will be applied. If there are no saved parameters, the factory-default configuration is loaded.
- The S2W application is initialized based on the profile settings.

If auto connection is enabled, the interface will attempt to associate with the specified network, previously set by the user (see [3.21.1 Wireless Parameters, page 252](#)). Once associated, it will establish a TCP or UDP connection within the specified parameters. If successful, the interface will enter the Auto Connect mode, where all data received on the serial port is transmitted to the network destination and vice versa.

If auto-connection is disabled or fails, the interface enters the command processing state.

Figure 2 Operating Modes of the Adapter



Upon power-up, the UART interface defaults to 9600 baud, using 8 bit characters with no parity bits and one stop bit. Similarly SPI interface defaults to Mode#0 (CPL=0, CPH=0). Any changes to this configuration that were made in a previous session using the ATB command (see [3.4.1 UART Parameters, page 65](#)) will be lost when power is lost. To make changes in the UART/SPI parameters that will persist across power cycling, the relevant changes must be saved into the power-on profile using AT&W (see [3.9.1 Save Profile, page 87](#)) and AT&Y (see [3.9.3 Selection of Default Profile, page 89](#)).

2.1.1 Network Configuration

Once associated, the adapter supports instances of four types of network entities: TCP client, TCP server, UDP client and UDP server. Each client, or server, is associated with one or more of a possible 16 **Connection Identifiers**, where the CID is a single hexadecimal number. More than one such entity can exist simultaneously; and a TCP server can have multiple connections, each with its own CID. When the adapter is in Auto Connect mode (see [3.21 Auto Connection, page 252](#)), the entity called for by the Profile is created automatically upon startup. In Command modes, servers and clients are created using specific serial commands (see [3.12.25 Gratuitous ARP, page 176](#)).

A TCP client ([Figure 3, page 29](#)) is created with the serial command AT+NCTCP (see [3.13.2 Get Network Interface Filter Configuration, page 179](#)). The client attempts to create a TCP network connection with the destination IP address and port specified within the command. If successful, it issues a CONNECT response with the CID of the client. Data

can then be sent to the remote server using the <ESC>S sequence (see 2.3 Data Handling, page 40) with the appropriate CID. Data from the server is passed back to the Host, with the CID to identify its source.

Figure 3 Creation and Use of a TCP Client

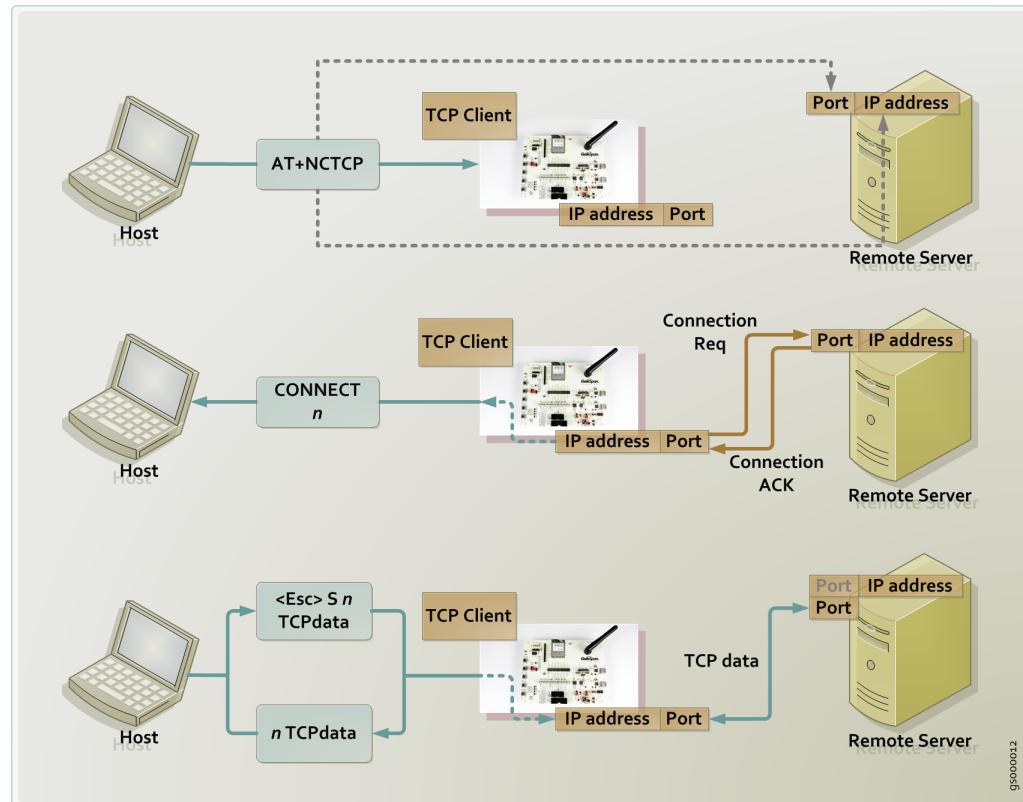
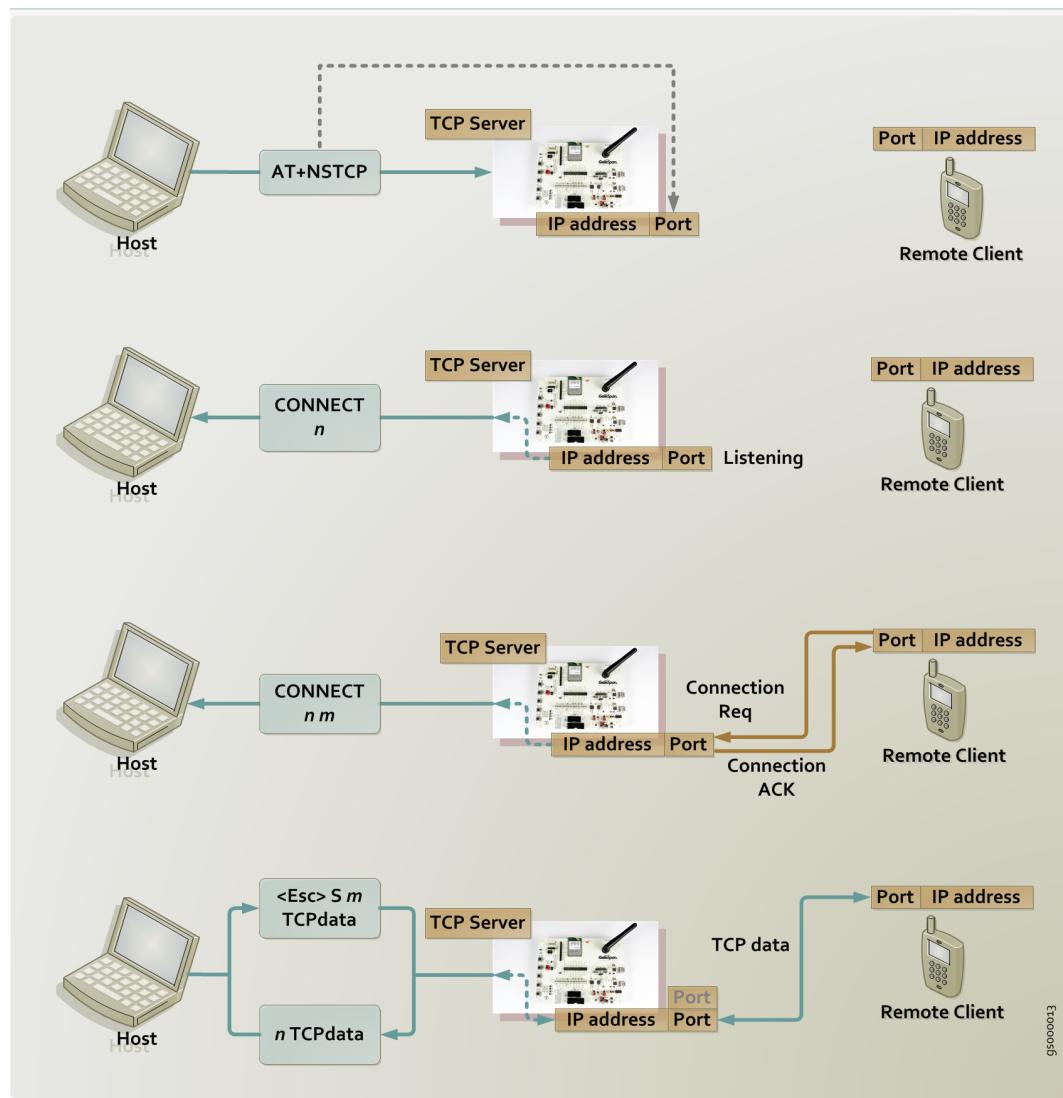


Figure 4, page 30 shows the corresponding sequence for a TCP server. A server is created with the serial command AT+NSTCP; it receives a CID, but listens passively until a remote client requests a connection. If that connection is successfully created, a second CONNECT message and a new CID are provided to the Host. It is this second CID that is used to send data to the remote client and identify received data from that client. A TCP server may support multiple clients, each with a unique CID.

Figure 4 Creation and Use of a TCP Server



A UDP client's life is depicted in Figure 5, page 31. The client is created with the serial command AT+NCUDP and receives a CID. The UDP client is associated with a specific destination port and address.

Figure 5 Creation and Use of a UDP Client

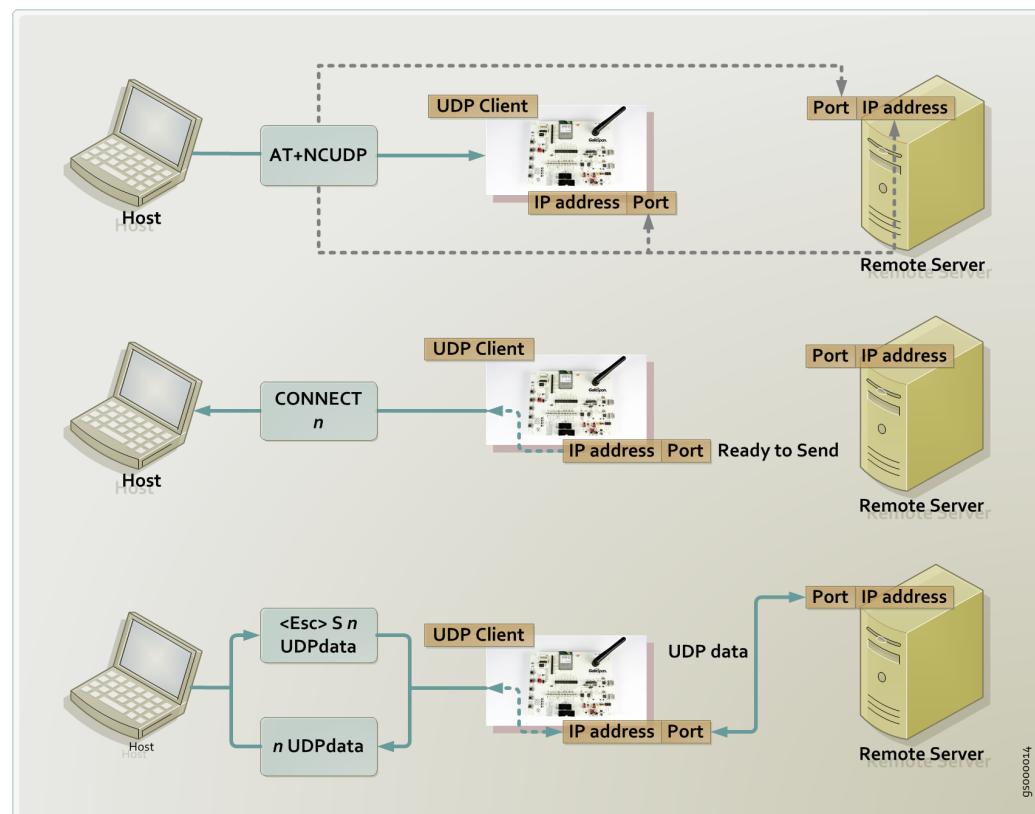
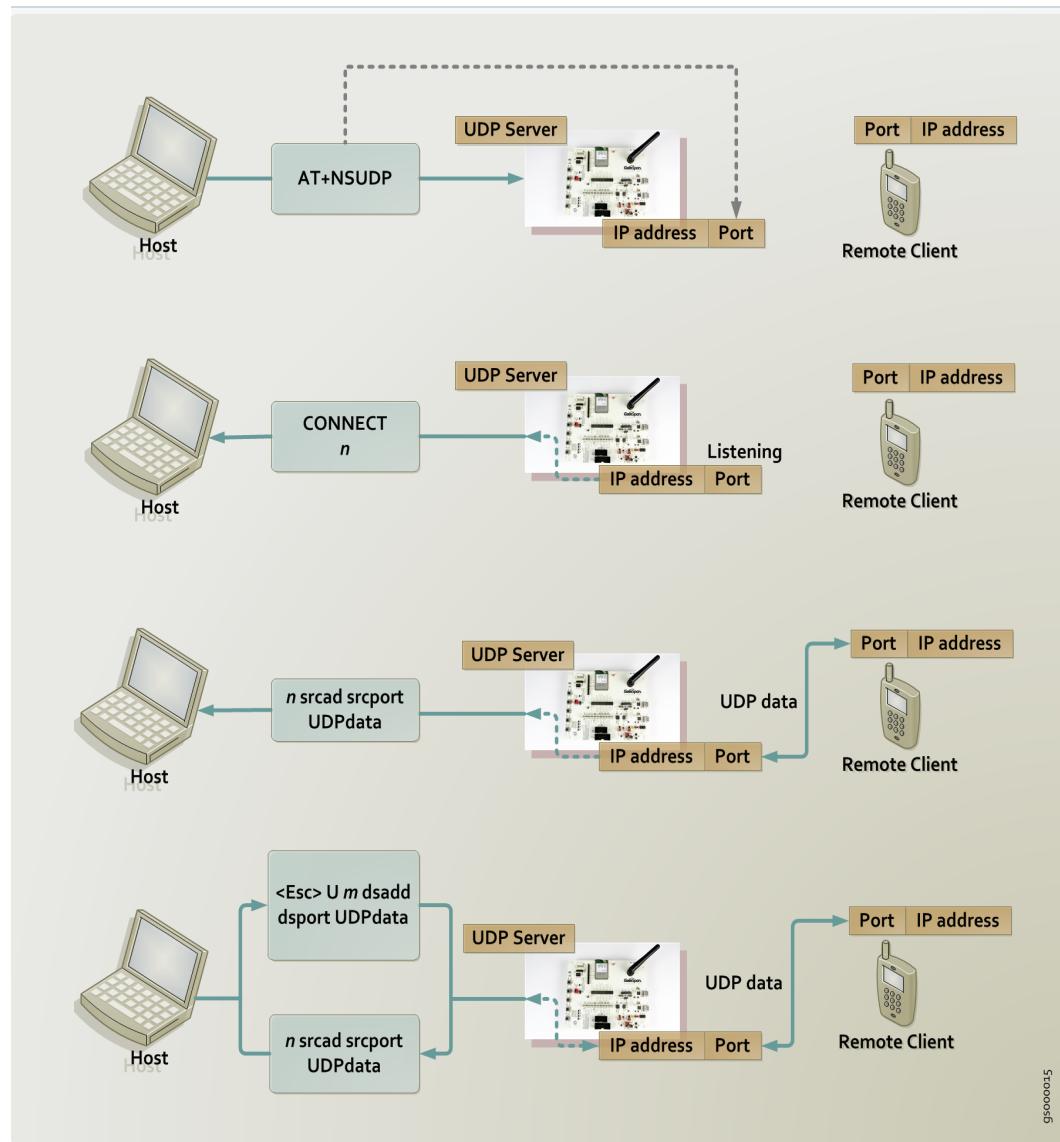


Figure 6, page 32 shows a UDP server. The server is created with AT+NSUDP and is assigned a CID. Individual clients do not receive unique CIDs; data sent using the UDP server must be accompanied with the destination IP address and port, and data received via the server is modified with the identifying source address and port number.



NOTE: When the CID returns for a new TCP/IP connection it should be in ascending order (incremented by 1) even the previous connection does not exists. Once it reaches the maximum connection number (15), it starts from the first (0).

Figure 6 Creation and Use of a UDP Server



95000000

2.1.2 Profile Definition

The configuration parameter values that define the behavior of the Adapter are grouped into Profiles. These profiles are stored in non-volatile memory when not in use. The default configuration supports single Profile. The contents of a profile are listed in [Table 9](#), page 33.

Table 9 Profile Definition Parameters

Parameter	Values	Reference
General Wireless Parameter		
802.11 Operating Mode	STA, Limited AP	2.6.1 Scanning, page 50
Transmit Power Configuration		N/A
802.11 Transmit Retry Count		3.10.17 Set Retry Count, page 113
Power Save Mode	Enabled, Disabled	3.11.15 Radio Receiver in Power Save Mode, page 133
802.11 Radio Mode	Enabled, Disabled	3.11.14 Radio Receiver in Active Mode, page 132
Auto Connect Mode, Wireless Interface Settings		
802.11 Operating Mode	STA	3.21.1 Wireless Parameters, page 252
Operating Channel	1 to 14	
SSID Parameter	Any valid SSID	
BSSID Parameter	Any valid BSSID	
Maximum Scan Time		3.7 Serial-to-WiFi Configuration, page 84
Auto Connect Mode, Network Interface Settings		
Mode	Server, Client	3.12.1 DHCP Client Support for IPv4, page 144
Protocol	TCP, UDP	
Server Port Number	Any valid port	
Server IP Address	Any valid IP address	
Host Name	Valid Domain name	
Wireless Interface Security Configuration		
Authentication Mode	Open, Shared	3.11.1 Authentication Mode, page 115
PSK Valid	Valid, Invalid	3.11.6 WPA-PSK and WPA2-PSK Key Calculation, page 120
PSK-SSID	Any valid SSID, used for PSK key computation	
WEP Key Configuration		3.11.2 Security Configuration, page 116
WPA Pass Phrase		3.11.5 WPA-PSK and WPA2-PSK Passphrase, page 118
TCP/IP Configuration		
DHCP Mode	Enabled, Disabled	3.12.1 DHCP Client Support for IPv4, page 144

Table 9 Profile Definition Parameters (Continued)

Parameter	Values	Reference
IP Address	Valid IP address	3.12.2 Static Configuration of Network Parameters for IPv4, page 147
Net Mask Address	Valid mask	
Default Gateway Address	Valid IP address	
DNS1	Valid DNS1 IP address	3.12.15 Static Configuration of DNS (Client), page 167
DNS2	Valid DNS2 IP address	
UART Configuration		
Echo Mode	Enabled, Disabled	3.2.2 Echo, page 62
Verbose Mode	Enabled, Disabled	3.2.3 Verbose, page 63
Bits Per Character	5, 6, 7, 8	3.4.1 UART Parameters, page 65
Number of Stop Bits	1, 2	
Parity Type	None, Odd, Even	
Software Flow Control Mode	Enabled, Disabled	3.4.2 Software Flow Control, page 66
Hardware Flow Control Mode	Enabled, Disabled	3.4.3 Hardware Flow Control, page 66
Baud Rate		3.4.1 UART Parameters, page 65
Limits and Timeouts		
Network Connection Timeout	Units of 10 milliseconds	3.7 Serial-to-WiFi Configuration, page 84
Auto Association Timeout	Units of 10 milliseconds	
TCP Connection Timeout	Units of 10 milliseconds	
Association Retry Count	Units of milliseconds	
Nagle Wait Time	Units of 10 milliseconds	
Scan Time	Units of milliseconds	
NCM L4 Reconnect Interval	Units of milliseconds	
NCM L4 Reconnect Count	Units of numbers	
SPI Configuration		
SPI Clock Polarity and Clock Phase	0, 1	3.5 SPI Interface and Configuration, page 68

2.2 Command Processing Mode

In **Command mode**, the application receives commands over the serial port. Commands are processed line by line.

Verbose Mode is used when referring to commands being executed, refers to the displaying of status of any command executed in ASCII (human readable) format. When the **Verbose Mode** is disabled, the output will simply be in numeric digits, each digit indicating a particular status. **Verbose Mode** is enabled by default.

If **echo** is enabled then each character is echoed back on the serial port.

Each command is terminated with a **carriage return** <CR> or **line feed** <LF>.

Each response is started with a **carriage return** <CR> and **line feed** <LF>, with the exception of the responses to the following commands:

The response to the following group of commands starts with a **line feed** <LF> only:

AT+WA

AT+NSTAT

AT+WPAPSK=<SSID>, <Passphrase>

AT+NSET=<IP Address>, <Subnet Mask>, <Gateway IP Address>
(valid after association)

AT+TRACEROUTE=<IP Address>

AT+PING=<IP Address>

ATA

AT+NDHCP (after association)

The response to the following group of commands starts with a **line feed** and **carriage return**: <LF><CR>:

AT+HTTPOPEN=<IP Address>

Unless otherwise specified, if **Verbose Mode** is enabled, then the response to a successful command is the characters **OK**. The response to an unsuccessful command is the word **ERROR**, followed by a detailed error message, if available. If verbose mode is disabled, command responses are numerical with **OK** having a value of 0 and error codes represented by positive integers.

The commands are described in [Chapter 3 Commands for Command Processing Mode, page 59](#).

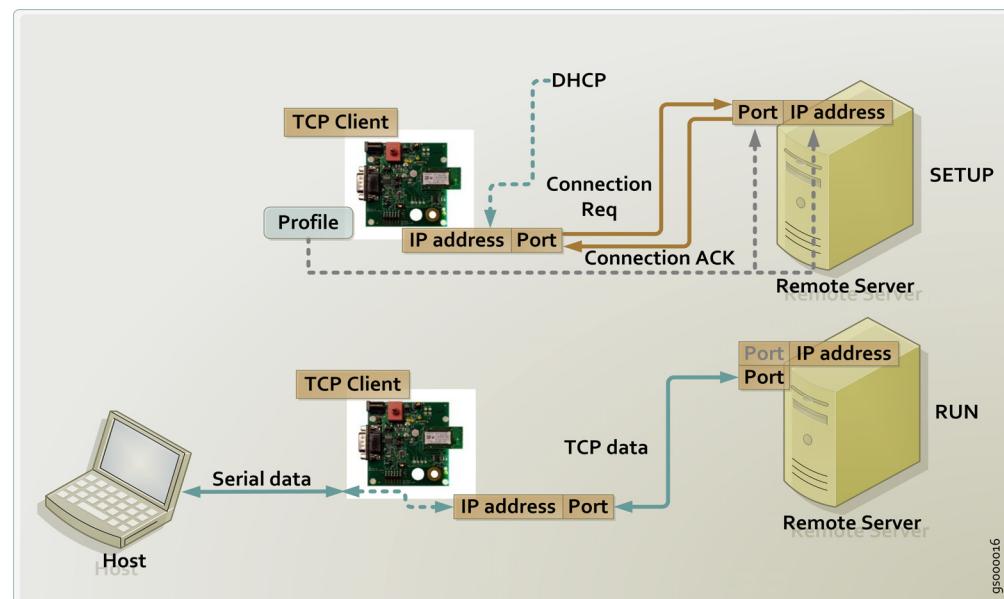
2.2.1 Auto Connection

If auto connection is enabled, then upon startup the Adapter will:

1. Attempt to associate to or from the specified network, for a maximum time of *Auto Associate Timeout* (see [3.7 Serial-to-WiFi Configuration, page 84](#)).
2. On successful association, attempt to establish a network connection based on the specified parameters.
3. On successful connection establishment, enter the pass-through auto connect mode
4. On failure, enter the command processing state.

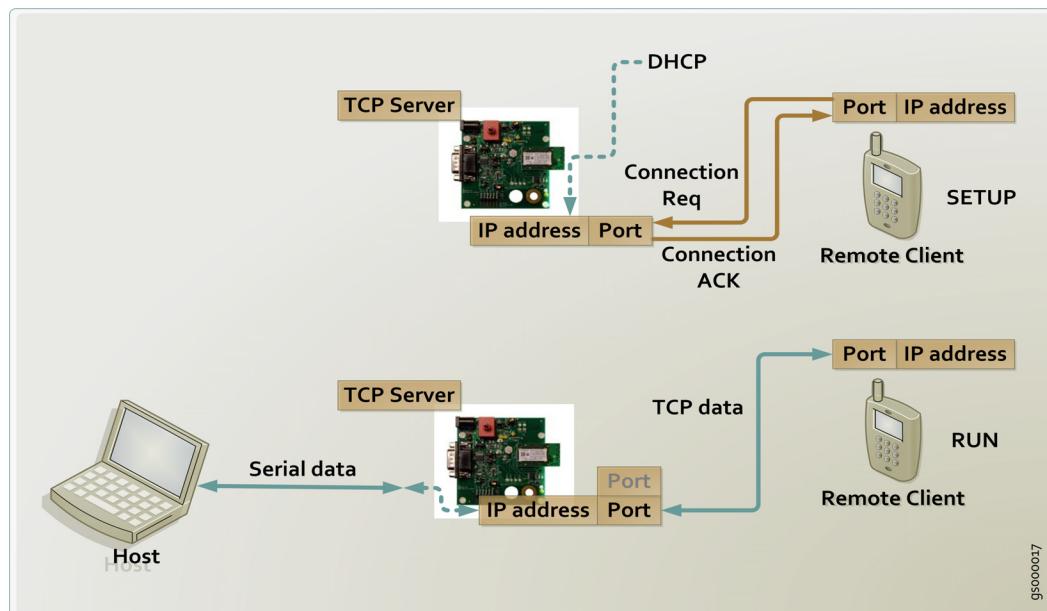
In **TCP client mode**, the connection is considered established only when the client successfully connects to the server specified in the parameters. The client address may be fixed or obtained from a DHCP server. The client port is selected at random during creation of the client. The connection is attempted for a maximum time based on the *Network Connection Timeout*, specified in units of 10 milliseconds (see [3.7 Serial-to-WiFi Configuration, page 84](#)). Data is sent to, and received from, this server. If the connection is terminated, auto-connect mode also terminates and the command processing state is entered (see [Figure 7, page 36](#)).

Figure 7 TCP Client Operation in Auto Connect Mode



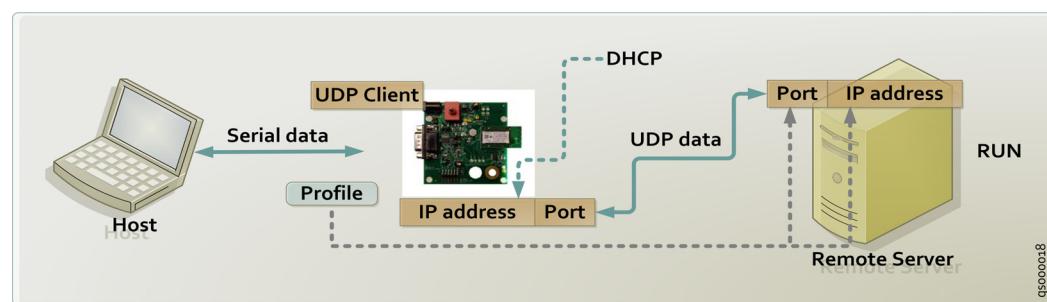
The TCP server IP address may be fixed in the profile or obtained from DHCP. The port for connection attempts to be made is obtained from the profile. In TCP server mode, the connection is considered established when the first client connects to the server. Data is sent to, and received from, this client. If the client disconnects, the adapter waits for the next client to connect (see [Figure 8, page 37](#)).

Figure 8 TCP Server Operation in Auto Connect Mode



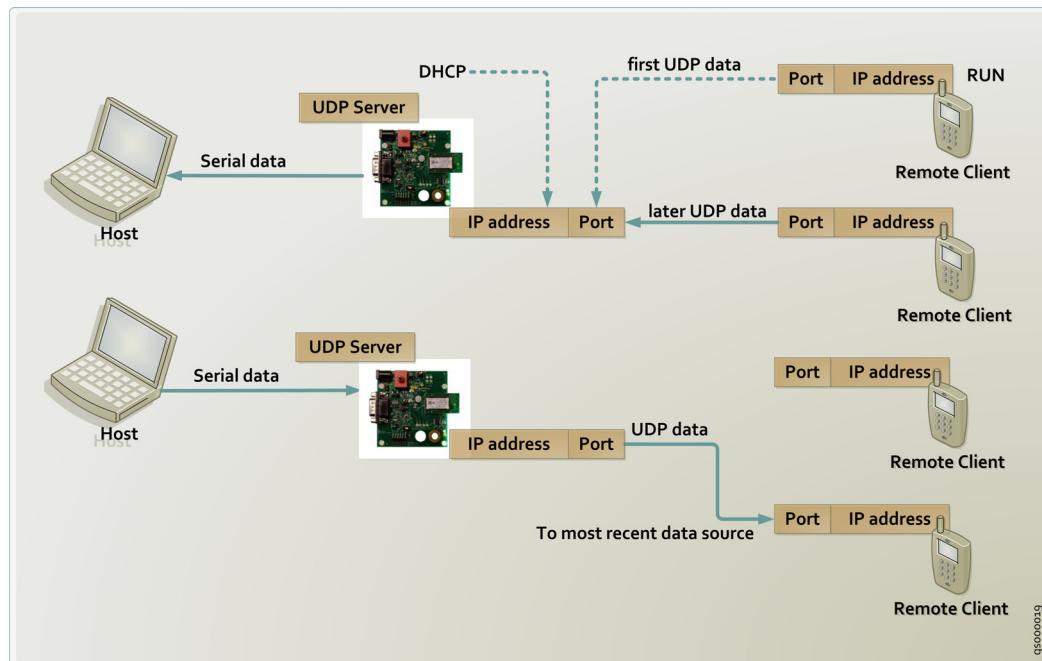
In **UDP client mode**, the connection is considered established when the client is created. The client IP address may be fixed or obtained from DHCP. The client port number is set at random upon creation of the client. Data is sent to and received from the configured server (see [Figure 9, page 37](#)).

Figure 9 UDP Client Operation in Auto Connect Mode



In **UDP server mode**, the connection is considered established when data is received from any client. The UDP server IP address may be fixed or obtained in DHCP. The port is set by the profile. Data received from any client is output on the serial port and data received on the serial port is transmitted to the client based on the last packet received (see [Figure 10](#)).

Figure 10 UDP Server Operation in Auto Connect Mode



In **TCP and UDP server mode**, even where no connection is established, the serial host may take control of the Serial-to-WiFi interface by issuing a specific escape sequence, described in [2.2.1.1 Auto Connection Operation, page 38](#).

2.2.1.1 Auto Connection Operation

The **Auto Connect Mode** acts as a cable replacement so that the interface acts like a serial interface. The node automatically establishes the wireless and network connections by using parameter values from the current active Profile and transfers data transparently between the Host and Target in data mode. No status information is sent to the Host. If connection is lost, status is sent to the Host, and host will need to re-initiate the connection to the network.

In auto connection mode the Adapter:

- Receives characters from the serial port and transmits them over the WiFi connection
- Receives data from the WiFi connection and transmits it on the serial port

The serial host may gain control of the interface by issuing the **escape sequence** “+++”, followed by a one-second gap where no characters are received on the serial port or by asserting GPIO8. When this sequence is encountered, the Adapter suspends auto connection mode and resumes command processing. The Host then may make changes in the network configuration or other parameters as needed. However, the Adapter does not accept any new TCP/UDP client/server or auto connection requests since auto connection exists in the background. The **AUTO** command (terminated by the ASCII character “O”, not the number 0) is used to return to auto connection mode.

In auto connection mode, the Nagle Algorithm Wait Time (see [3.7 Serial-to-WiFi Configuration, page 84](#)) can be used to buffer any characters to be sent, in order to avoid sending a large number of packets with small payloads onto the network. The wait time is specified in units of 10 milliseconds. This functionality is available for both UDP and TCP connections.

NCM runs in the background so that if there is disconnection on L2/L3/L4, the NCM re-establishes the connection without any message to the host.

Here, the host checks whether the GPIO19 is high to send data via the data pipe created by auto connection.

When L2, L3, or L4 disconnects, GPIO19 goes low and the host stops sending data via the data pipe created by auto connection.

2.3 Data Handling

In **Data Processing Mode**, data transfers are managed using various *escape sequences*. Each escape sequence starts with the ASCII character 27 (0x1B); this is equivalent to the ESC key. The encoding of data and related commands are described in the following pages. This encoding is used for both transmitted and received data.

The network destination, or destination source, for a given data packet is established by means of a **Connection Identifier**, and represented as a single hexadecimal number. Data is transferred on a per CID basis. Data is normally buffered until the end-of-data escape sequence is received. However, if the amount of data exceeds the size of the data buffer, the data received, thus far, is sent immediately. The data buffer size depends on the implementation, but is usually one MTU (1400 bytes).

The process of sending a data packet is depicted in [Figure 11, page 41](#). The sequence ESC S or ESC U is sent to initiate the data transfer. This sequence is followed by a single-digit CID; if the CID is valid, the subsequent characters are assembled into a data stream, terminated by ESC E, ESC C, ESC S or ESC U. With a terminating sequence, the data is sent via the requested network connection and the system either returns to command processing or to further data processing.

Escape <ESC> sequences like ESC H, ESC S, ESC u and ESC U support only ASCII data handling while ESC Z, ESC Y and ESC y supports all types of data (ASCII, Binary etc.) handling.

Refer to [Appendix A Data Handling Escape Sequences, page 319](#) for a complete description of all the Escape <ESC> sequences used for data handling (see [Table 10, page 42](#)).

Figure 11 Data Processing Flow

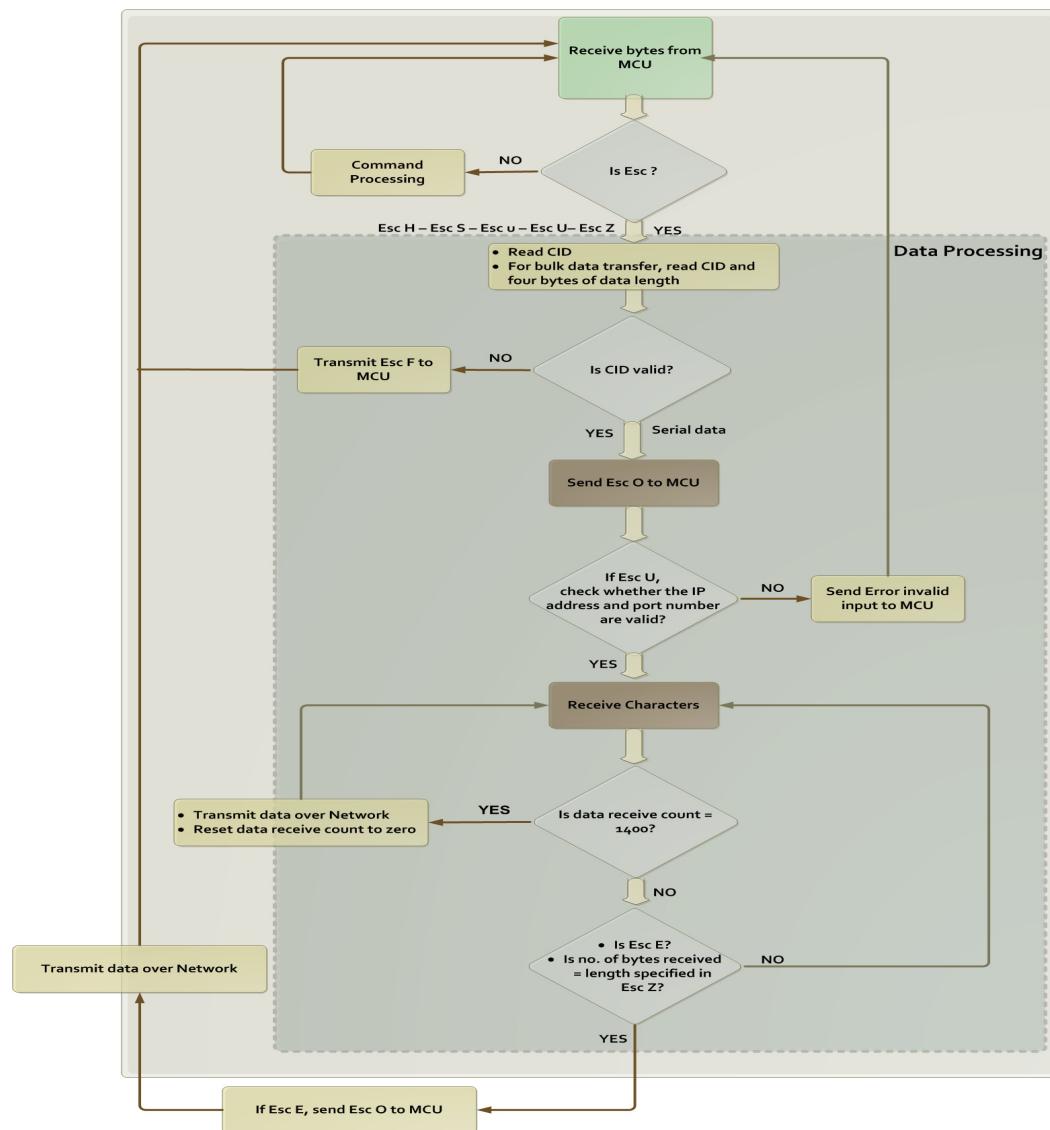


Table 10 Data Handling Responses at Completion

Operation	Escape Sequence	Description
Send and Return to Command Mode Sequence	<ESC>C	This sequence causes transmission of the data received on the serial interface on a TCP server/client or UDP client connection. After, the currently selected connection is closed and the interface returns to Command mode. Any buffered data is sent before the connection is closed. This can be issued from the serial host once the data transmissions start on a socket using <ESC>S<CID> sequence.
Success Indication	<ESC>O	OK: When serial host sends data to any socket, the network validates whether it is an active CID. This sequence is sent to the serial host through UART or SPI-NON DMA interface by the Serial-to-WiFi Adapter upon successful validation of active CID. Note: Sending <ESC> O has been intentionally removed in SPI DMA and SDIO interface to increase throughput.
Failure Indication	<ESC>F	FAILURE: This sequence is sent to the serial host by the Serial-to-WiFi Adapter through all interfaces (UART, SPI-NON DMA, SPI-DMA) when serial host sends data to any invalid socket.



NOTE: The contents of < > are either a byte or byte stream, except for <ESC>; literals outside brackets are ASCII characters.

2.3.1 Bulk Data Tx and Rx

In **Bulk Data Mode**, data transfers are managed using **escape sequences (ESC Z, ESC Y and ESC y)**. Each escape sequence (see Table 11, page 43) starts with the Escape <ESC> key (ASCII character 27 (0x1B)). Encoding is used for both transmitted and received data. Enable bulk data by using command “AT+BDATA=” (1 is enable and 0 is disable).

The format of a bulk data frame for TCP client, TCP server, or UDP client is:

```
<ESC>Z<CID><Data Length xxxx 4 ascii char><data>
```

The contents of < > are a byte or byte stream.

- CID is connection identifier (UDP, TCP, etc.; as derived when TCP socket is created by issuing the command: AT+NCTCP, for example.)

- Data Length is 4 ASCII character represents decimal value i.e. 1400 byte (0x31 0x34 0x30 0x30).
- The Data Length range should be 1 to 1400 bytes when sending to GainSpan module from Host and it will be 1 to 1500 bytes when Host is receiving from GainSpan module

User Data size **must match** the specified Data Length. Ignore all command or Escape <ESC> sequence in between data pay load. User should send the specified length of data to the adapter irrespective of any asynchronous events happened on the adapter so that the adapter can start receiving next commands.

For example, if CID value is 3, then:

To send a 5 byte user data (e.g. ABCDE) for a TCP client connection, the format will be:

```
<ESC>Z30005ABCDE
```

To send a 512 byte user data for a TCP client connection, the format will be:

```
<ESC>Z30512<512 bytes of user data>
```

To send data on UDP server, the bulk data frame format is:

```
<ESC>Y<CID><Ip address>:<port>:<Data Length xxxx 4 ascii char><data>
```

When receiving data on UDP server, the format of a bulk data frame is:

```
<ESC>y<CID><IP address><space><port><horizontal tab><Data Length xxxx 4 ascii char><data>
```

Table 11 Escape Sequences

Operation	Escape Sequence	Description
Bulk Data transfer on TCP Server/Client and UDP Client connection	<ESC>Z<CID>Data Len 4 digit ascii<Data>	To improve data transfer speed, one can use this bulk data transfer. This escape sequence is used to send and receive data on a TCP Client/Server and UDP client connection.
Example: <ESC>Z40005Hello - where 4 is the CID, 0005 is the 5 byte data length and Hello is the data to be sent.		
Bulk Data Send on UDP server connection	<ESC>Y<CID>remote address : remote port : Data Len 4 digit ascii<Data>	This escape sequence is used when sending UDP data on a UDP server connection. When this command is used, the remote address and remote port is transmitted in ASCII text encoding and terminated with a ":" character.

Table 11 Escape Sequences (Continued)

Operation	Escape Sequence	Description
Example: <ESC>Y4192.168.1.52:000Hello where 4 is the CID, 0005 is the 5 byte data length and Hello is the data to be sent.		
Bulk Data Receive on UDP Server Connection	<ESC>y<CID>remoteaddress<space>remote port<horizontal tab>Data length in 4 digit ascii<Data>	This escape sequence is used when receiving UDP data on a UDP server connection. When this sequence is used, the remote address and remote port is transmitted in ASCII text encoding and separated by a space () character.
Example: <ESC>y4192.168.1.1<space>53<horizontal tab>0005Hello where 4 is the CID, 0005 is the 5 byte data length and Hello is the data received.		

**NOTE:**

a> The contents of < > are either a byte or byte stream, except for <ESC>; literals outside brackets are ASCII characters.

b> GS module sends success or failure responses as mentioned in [Table 10 Data Handling Responses at Completion when MCU transmits bulk data](#).

2.3.2 Unsolicited Data Handling

In **Unsolicited Data Mode** (data transmission without association), data transfer is managed using *escape sequences*. Each escape sequence starts with the ASCII character 27 (0x1B), equivalent to the Escape <ESC> key. The encoding of data is described below. This encoding is used for transmitted data only. The unsolicited data transmission Enable command (see [3.14 Unassociated Frame Transmission and Reception, page 214](#)) must be issued before sending unsolicited data through the Adapter.

The format of an unsolicited data frame is:

<ESC>D/d<Payload>

The Payload contents are byte or byte stream.

2.3.3 Software Flow Control

The **Software Flow Control** (for UART interface) works only with ASCII data transfers and cannot be used for binary data. For SPI interface and use of flow control.

If software flow control is enabled, and the interface receives an XOFF character from the serial host, it stops sending to the host until it receives an XON character. If the Adapter is receiving data over the wireless connection during the time that XOFF is enabled, it is possible for the wireless buffer to become full before XON is received. In such a case, data from the network will be lost.

If software flow control is enabled, then the interface sends an XOFF character to the host when it will be unable to service the serial port. The XON character is sent when the interface is once again able to accept data over the serial port.



NOTE: *With initialization, the Adapter treats the serial channel as clear with no restrictions on data transmission or reception; no explicit XON by the Adapter or required from the Host, even if flow control is enabled.*

2.3.4 Hardware Flow Control

The Hardware Flow Control is a handshake mechanism between the Serial host and S2W adapter on UART interface, using two additional CTS and RTS connections. This feature prevents the UART hardware FIFO overflow on S2W adapter due to high speed data transmission from/to the S2W adapter. If hardware flow control is enabled, an RTS/CTS handshake will occur between the serial host and the Adapter. This is a hardware feature and available only for UART interface.

The S2W adapter uses both CTS and RTS signals as “low” to indicate the readiness to send or receive data from serial host.

2.4 Serial Data Handling

The **Serial Data Handler** receives and transmits data to and from the hardware serial controller. Data read from the serial port is passed to:

- The command processor in command mode
- The Tx data handler in data mode
- The auto connection mode processor for data transfer in auto connection mode

Then Data is transferred on the serial port from:

- The command processor in order to output responses to commands
- The Tx data handler in order to output incoming packets
- The Rx data handler in order to output incoming packets
- The auto connection handler in order to output incoming data
- The connection manager in order to output status indications
- The wireless connection manager in order to output status indications

When configured in **Auto Connection Mode**, the Adapter enters directly into **Data Processing Mode** after the completing the connection without sending any status information to the Host.

2.5 Connection Management

The **Connection Management** module is responsible for processing connection-related events. The interface provides UDP and TCP sockets (similar to the familiar BSD network sockets). Each socket may represent either a server or client connection. Each connection has a unique, single-digit hexadecimal value (0 to F), for the CID.



NOTE: *This single pool of CIDs is used for TCP, UDP, Server, and Client connections.*

2.5.1 Packet Reception

When a packet is received on any open connection, and the application is not currently in auto-connect mode, the packet is transferred on the UART/SPI in the form described in [2.3 Data Handling, page 40](#). Received data payloads are encoded with the appropriate Escape <ESC> sequence. The connection ID is used to inform the serial host of the origin of an IP data packet. The source IP address and port are provided along with the data when a UDP packet is received.

If auto-connect mode is enabled and a packet is received on the auto-connected CID, the packet data is sent without modification over the UART/SPI to the serial host.

2.5.2 Remote Close

If a TCP connection is terminated by disconnection from the remote end, an unsolicited ASCII-format response of the form DISCONNECT Connection ID is sent to the serial host, and the specified CID should be considered unavailable. If the connection ends because the remote server has shut down, the unsolicited response ERROR:SOCKET FAILURE Connection ID will be sent to the host.



NOTE: *A data packet from the remote client or server containing the same ASCII characters CLOSE Connection ID is treated as data rather than a command and forwarded to the serial host.*

2.5.3 TCP Server Connections

Upon deployment of incoming TCP connections on a socket, the incoming connection is allowed if the limit on the maximum number of connections has not been reached.

There is an unsolicited response of the form:

```
CONNECT <server CID> <new CID> <ip> <port>, where:
```

- server CID is the CID of the server where the connection has arrived
- new CID is the CID allocated for this client connections
- ip and port is the IP and Port of the client encoded in the binary encoding used for UDP server data packets described in [2.3 Data Handling, page 40](#) above is sent to the serial host. The host can use the IP address to ascertain the source of the TCP connection request. The TCP server has no timeout limitation for an incoming connect request. It waits indefinitely, until a CLOSE command is received.



NOTE: If Verbose mode is disabled (see [3.2.3 Verbose, page 63](#)), the word CONNECT in the unsolicited response is replaced by the number 7.

2.6 Wireless Network Management

2.6.1 Scanning

The Serial-to-WiFi interface can instruct the WiFi radio to scan for access points with a specified SSID, BSSID and/or channel for a specified scan time. Scanning can be performed to find networks with a specific SSID or BSSID, networks operating on a specific radio channel or a combination of these constraints.

2.6.2 Association

The Serial-to-WiFi interface performs all the actions required to join an infrastructure IP network:

- Scan for a specific AP (AT+WS) – see [3.10.7 Scanning, page 98](#)
- Authenticate the specified network using the configured authentication mode (AT+WAUTH) – see [3.11.1 Authentication Mode, page 115](#) for more information
- Associate to the AP (AT+WA) – see [3.10.9 Associate with or Create an Infrastructure \(AP\) Network, page 102](#)
- Perform security negotiation if required
- Change state to Wireless Connected
- Initialize the networking stack using the configured static IP address or via DHCP (AT+NDHCP) – see [3.12.1 DHCP Client Support for IPv4, page 144](#)

2.6.3 SSID and Passphrase

The following rules apply:

1. The S2W Adapter accepts the following ASCII characters for SSID and passphrase (see [Table 12, page 51](#)).

Table 12 SSID and Passphrase Characters

Category	Accepted Characters
Numerical	0-9
Alphabets	a-z and A-Z
Special Characters	¹ SP ! # \$ % & ' () * + , - . / ; < = > ? @ [\] ^ _ ` { } ~ "

Note: 1. SP = space.

2. The SSID or Passphrase parameter may be captured within or without double quotation marks (“SSID”).
3. The quotation mark (“”) may not be used as the first character of the SSID or passphrase.
4. If comma (,) is a part of the SSID, then SSID parameter needs to be framed with double quotation marks (“SS, ID”) (see [Table 13, page 51](#)).

Table 13 Expected and Input SSID

Expected SSID	Input SSID	Remarks
TEST	TEST	Valid (satisfies rule 2)
TEST	“TEST”	Valid (satisfies rule 2)
TE”ST	TE”ST	Valid (satisfies rule 3)
TE”ST	“TE”ST”	Invalid (breaks rule 3)
TE,ST	“TE,ST”	Valid (satisfies rule 4)
TE,ST	TES,T	Invalid (breaks rule 4)
TE,S”T	“TE,S”T”	Invalid (breaks rule 3 and 4)

2.7 Response Codes

The possible responses sent by the Adapter to the serial host are categorized as follows:

- **Synchronous messages**
- **Asynchronous messages**
 - Enhanced asynchronous messages
 - Exception messages
 - Boot messages

Table 14, page 52 lists the response codes with all characters including: <CR> or <LF> that would be seen on the MCU interface.

Table 14 Response Codes

No.	ASCII Character	Response	ASCII String	Meaning
Synchronous Messages				
1	0	S2W_SUCCESS	"\r\nOK\r\n"	Command Request Success
2	1	S2W_FAILURE	"\r\nERROR\r\n"	Command Request Failed
3	2	S2W_EINVAL	"\r\nERROR: INVALID INPUT\r\n"	Invalid Command or Option or Parameter
4	4	S2W_ENOCID	"\r\nERROR: NO CID\r\n"	GS node support only 16 CIDs, it will not create the next connection (i.e., 17 th connection) when all 16 CIDs are being active.
5	5	S2W_EBADCID	"\r\nERROR: INVALID CID\r\n"	Invalid Connection Identifier
6	6	S2W_ENOTSUP	ERROR:NOT SUPPORTED	Operation not supported
7	7	S2W_CON_SUCCESS	"\r\nCONNECT <CID>\r\n\r\nOK\r\n"	GS node TCP/IP server created successfully or GS node TCP/IP client connected to an external TCP/IP server successfully. where <CID> = TCP server's CID in hexadecimal format It is followed by command request success.

Table 14 Response Codes (Continued)

No.	ASCII Character	Response	ASCII String	Meaning
8	9	S2W_LINK_LOST	"\r\nDISASSOCIATED\r\n"	GS node is not associated to a wireless network. Example: If a GS node is no longer associated to any AP and MCU sends commands such as AT+NCTCP/UDP or AT+NSTCP/UDP, then DISASSOCIATED response code is returned to MCU.
Asynchronous Messages				
1	3	S2W_SOCK_FAIL	"\r\nERROR: SOCKET FAILURE <CID>\r\n"	Socket Operation Failed. The network connections are closed automatically after the reception of this response.
3	8	DISCONNECT <CID>	"\r\nDISCONNECT <CID>\r\n"	TCP/IP connection with the given CID is closed. This response is sent to the host when a network connection is closed by the remote device.
4	10	S2W_DISASSO_EVT	"\r\n\r\nDisassociation Event\r\n\r\n"	Wireless network association lost
5	11	S2W_STBY_TMR_EVT	"\r\n\r\n\r\nOut of StandBy-Timer\r\n\r\n"	Wake up from Standby due to RTC timer expiration.
6	12	S2W_STBY_ALM_EVT	"\r\n\r\n\r\nOut of StandBy-Alarm\r\n\r\n\r\n"	Wake up from Standby due to receipt of an Alarm signal
7	13	S2W_DPSLEEP_EVT	"\r\n\r\n\r\nOut of Deep Sleep\r\n\r\n\r\nOK\r\n\r\n"	Wake from Deep Sleep followed by command request success
8	15	S2W_ENOIP	"\r\nERROR:\ IP CONFIG FAIL\r\n"	IP configuration has failed. This message comes asynchronously when there is a DHCP renew failure.
9	16	Boot Message	"\r\nSerial2WiFi APP\r\n"	Initial Boot message
11	18	Nwconnection success	"\r\nNWCONN-SUCCESS\r\n"	The L2+L3 connection success message for the NCM auto connection.
12	19	S2W_NEWINP	"\r\nIP CONFIG-NEW IP\r\n"	DHCP renewal success with a new IP address
13	17	Boot Message	"\r\n\r\nExternal Reset Boot\r\n\r\n"	Boot message for the MCU when reset is triggered from external reset pin.

Table 14 Response Codes (Continued)

No.	ASCII Character	Response	ASCII String	Meaning
14	31	IP conflict	"\n\rIP Conflict Detected\r\n"	IP conflict is detected.
15	20	Reset Message	"\r\n\r\n\rAPP Reset-Wlan-Wd\r\n\r\n"	Boot message for an adapter reset with WLAN watch dog
16	21	Reset Message	"\r\r\r\rAPP Reset-App-Wd\r\n\r\n"	Boot message for an adapter reset with Application watch dog
17	22	Reset Message	"\r\r\r\rAPP Reset-Wlan SW Reset\r\n\r\n"	Boot message for an adapter reset with WLAN reset
18	23	Reset Message	"\r\rAPP Reset-APP SW Reset\r\n"	Boot message for an adapter reset with Application reset
19	24	Reset Message	"\r\r\r\rAPP Reset-Wlan Except\r\n\r\n"	Boot message for an adapter reset with WLAN exception
20	25	Boot Message	"\r\rAPP Reset External Flash FW-UP-SUCCESS\r\r\r\n"	Boot message for an adapter reset with firmware update success

2.7.1 Enhanced Asynchronous Messages

Table 15, page 55 lists the enhanced asynchronous messages which is a subset of Response codes.

Table 15 Enhanced Asynchronous Messages

No.	Message	Subtype	Meaning
1	ERROR:SOCKET FAILURE <CID>	0	Socket Operation Failed The network connections are closed automatically after the reception of this response.
2	CONNECT <TCP SERVER CID><CLIENT CID><CLIENT IP ADDR><CLIENT PORT>	1	TCP/IP connection is successful where, <TCP SERVER CID> = server's CID in hexadecimal format <CLIENT CID> = client's CID in hexadecimal format <CLIENT IP ADDR> = client's IP address <CLIENT PORT> = client's port This is applicable when GS node is in Station mode.
3	DISCONNECT <CID>	2	TCP/IP connection with the given CID is closed. This response is sent to the host when a network connection is closed by the remote device.
4	Disassociation Event	3	Wireless network association with AP is lost. After association with an AP, if GS node is disconnected from the AP (AP is switched off or it is out of range); this message is sent to the MCU.
5	Out of Standby-Timer	4	Wake up from Standby due to RTC timer expiration. When GS node is in standby, only RTC clock will be running. MCU configures the standby time using RTC timer and will receive this message when the timer expires.
6	Out of Standby-Alarm	5	Wake up from Standby due to receipt of an Alarm signal. When GS node is in standby, only RTC clock will be running and hence RTC pins will be active. MCU configures the RTC alarm pin to activate GS node from standby. When the RTC alarm pin is enabled, the GS node comes out of standby and sends this message to MCU.
7	Out of Deep Sleep	6	Wake from Deep Sleep.
8	ERROR:IP CONFIG FAIL	8	IP configuration has failed. This message comes asynchronously when DHCP renew fails.
9	Serial2WiFi APP	9	Initial Boot message
10	ERROR	B	Error message for the L4 connection fail with NCM auto.

Table 15 Enhanced Asynchronous Messages (Continued)

No.	Message	Subtype	Meaning
11	NWCONN-SUCCESS	C	The L2+L3 connection success message for the NCM auto connection.
12	IP CONFIG-NEW IP	D	DHCP renewal success with a new IP address.
13	APP Reset-Wlan-Wd	E	Boot message for an adapter reset with WLAN watch dog.
14	APP Reset-App-Wd	F0	Boot message for an adapter reset with Application watch dog
15	APP Reset-Wlan SW Reset	F1	Boot message for an adapter reset with WLAN reset
16	APP Reset-APP SW Reset	F2	Boot message for an adapter reset with Application reset
17	APP Reset-Wlan Except	F3	Boot message for an adapter reset with WLAN exception
18	APP Reset External Flash FW-UP-SUCCESS	F4	Boot message for an adapter reset with firmware update success
19	External Reset Boot	F6	Boot message for an adapter reset with external reset pin
20	IP Conflict Detected	FA	IP conflict is detected

**NOTE:**

- a.) When verbose mode is disabled, an ASCII string gets replaced by its ASCII character.
- b.) MCU has to wait for an infinite time for a command response.
- c.) "\r\n" is appended to each asynchronous message and it is not included in the length.

2.7.2 Exception Messages

The possible exception messages sent by the Adapter to the serial host are enumerated in Table 16, page 57.

Table 16 Exception Messages

No.	ASCII String	Meaning
1	\r\n\r\n\rAPP Reset-Wlan SW Reset\r\n\r\n	Adapter reset due to WLAN processor software reset.
2	\n\rAPP Reset-APP SW Reset\r\n	Adapter reset due to app processor software reset. This can also be triggered when AT+RESET command is issued and in this case it is not considered an asynchronous message.
3	\r\n\r\n\rAPP Reset-Wlan-Wd\r\n\r\n	Adapter reset due to WLAN processor watchdog.
4	\r\n\r\n\rAPP Reset-App-Wd\r\n\r\n	Adapter reset due to app processor watchdog.
5	\r\n\r\n\rAPP Reset-Wlan Except\r\n\r\n	Adapter reset due to WLAN processor software abort or assert.

If the exception is due to one of the WLAN wd/SW Reset/Except, then the adapter send memory dump information of its WLAN registers to the serial host starts with the message \r\n---MEM-DUMP-START:\r\n and end with the message \n\r---MEM-DUMP-END:\r\n.



NOTE:

- a.) *Exception messages* a result of an undefined/unexpected behavior of the GS module that can occur at any time.
- b.) *All exception messages are sent after a module reset.*
- c.) *After reset due to exception message, GS module comes back to the saved profile state before reset.*

2.7.3 Boot Messages

The possible boot messages sent by the Adapter to the serial host are enumerated in [Table 17, page 58](#).

Table 17 Boot Messages

No.	ASCII String	Meaning
1	\r\nSerial2WiFi APP\r\n	Normal Serial-to-WiFi adapter boot message with internal PA. This boot message is also applicable when reset is triggered from external reset pin.
2	"\r\n\r\nExternal Reset Boot\r\n\r\n"	Boot message for the MCU when reset is triggered from external reset pin.
3	"\r\nAPP Reset External Flash FW-UP-SUCCESS\r\n\r\n"	Boot message for an adapter reset with firmware update success



NOTE:

- a.) If the asynchronous message format is enabled in the saved profile, the boot messages are sent in the asynchronous message format.
- b.) If the asynchronous message format is disabled in the saved profile, the boot messages are sent in the format of standard responses depending on the verbose mode.
- c.) After the boot message has been received, the GS module is ready for commands.

Chapter 3 Commands for Command Processing Mode

This chapter provides the GainSpan® AT Serial-to-WiFi commands used to configure and view system effects.

The following AT commands are described in this chapter:

- [Command Interface, page 62](#)
- [Node Start Up Handling , page 64](#)
- [UART Interface Configuration, page 65](#)
- [SPI Interface and Configuration, page 68](#)
- [Serial-to-WiFi Configuration, page 84](#)
- [Identification Information, page 86](#)
- [Serial-to-WiFi Profile Configuration, page 87](#)
- [WiFi Interface Configuration, page 92](#)
- [WiFi Security Configuration, page 115](#)
- [Network Interface, page 144](#)
- [Connection Management Configuration, page 177](#)
- [Unassociated Frame Transmission and Reception, page 214](#)
- [ISO TX, page 223](#)
- [GSLINK, page 225](#)
- [CoAP, page 235](#)
- [Using CoAP with GSLink, page 241](#)
- [Battery Check, page 242](#)

The following AT commands are described in this chapter (cont.):

- Power State Management, page 246
- Auto Connection, page 252
- Network Connection Manager (NCM), page 259
- Roaming, page 267
- Provisioning, page 269
- RF Tests, page 277
- Miscellaneous, page 292
- Over the Air Firmware Upgrade Using External Flash, page 303
- ADC Commands, page 306
- I2C Commands, page 311
- Pulse Width Modulation (PWM) Commands, page 314

3.1 Overview

Formatting and processing of commands is described in **Command Processing Mode**. Parameters are generally ASCII characters. For example, ATEn with n=1 is the series of ASCII characters ‘A’, ‘T’, ‘E’ , and ‘1’. Where some parameters are optional, mandatory parameters are denoted by <> and optional parameters by []. If a parameter is mandatory, any associated sub-parameters are also mandatory; sub-parameters of an optional parameter are optional. Parameters must always be provided in the order given in the command description. When an optional parameter is not supplied, the comma delimiters must still be included in the command. Every command starts with the characters “AT”; any other initial characters will cause an error to be returned.

Command Response: In most cases, valid commands return the characters OK if verbose mode is enabled and 0 verbose mode is not enabled. Invalid inputs return ERROR:INVALID INPUT if verbose is enabled and 2 if it is not. Exceptions to this rule are noted explicitly below.

3.2 Command Interface

3.2.1 Interface Verification

The command AT can be issued to verify that the interface is operating correctly or not.

Command Syntax AT

Synchronous Response

Table 18, page 62 describes the synchronous responses and remarks for the Interface Verification command.

Table 18 Interface Verification Synchronous Responses

Responses	Remarks
OK	Success

3.2.2 Echo

This command is used to enable or disable the echo back to host (MCU).

Command Syntax ATEn

Parameter Description

Table 19, page 62 describes the Echo parameters.

Table 19 Echo Parameters

Parameter	Value	Description
n	0	Disabled
	1 (default)	Enabled If echo is enabled, every character received from host (MCU) is transmitted back to host.

Note:

This is applicable only for this command.

When Echo command is enabled, ensure that:

- Host sends only one byte (either \r or \n) after any AT command.
- \r or \n is not sent after sending any data (bulk data or any data).

Example:

Send only AT+CID=?\r

Do not send AT+CID=?\r\n

Synchronous Response

Table 20, page 63 describes the synchronous responses and remarks for the Echo command.

Table 20 Echo Synchronous Responses

Synchronous Responses	Remarks
OK	Success
ERROR: INVALID INPUT	If parameters are not valid.

3.2.3 Verbose

This command is used to enable or disable verbose mode for synchronous and asynchronous responses.

Command Syntax `ATVn`

Parameter Description

Table 21, page 63 describes the Verbose parameters.

Table 21 Verbose Parameters

Parameter	Value	Description
n	0	Verbose response is disabled, the status response is in the form of numerical codes. For more information about the numerical codes when Verbose is disabled, refer to the ASCII Character column in Table 14 Response Codes .
	1 (default)	Enabled Verbose responses are enabled. The status response is in the form of ASCII strings.

Synchronous Response

Table 22, page 63 describes the synchronous responses and remarks for the Verbose command.

Table 22 Verbose Synchronous Responses

Responses	Remarks
OK	Success
ERROR: INVALID INPUT	If parameters are not valid. (n other than 0 or 1)

3.3 Node Start Up Handling

For proper synchronization between host micro controller (MCU) and S2W node, the following steps must be followed:

1. In case of UART interface:
 - a. MCU waits for the S2W start-up banner and issues commands only after receiving it completely.
 - b. If MCU misses the start-up banner, then it sends dummy ‘AT’ command and waits for response from the S2W node during boot up. MCU must continuously send these dummy ‘AT’ commands till ‘OK’ response is received from S2W node.
2. In case of SPI interface, host MCU must check the status of host wake-up signal (GPIO37 for GS2000 based modules) during boot up. Once host wake-up signal is HIGH, then the host must read the “Serial2WiFi APP” banner which is queued for transmission at the GainSpan node’s SPI interface at this point. To do so, it can simply repeatedly transmit idle characters (F5) over the SPI line and read the characters transmitted by the GainSpan node (“Serial2WiFi APP” banner) until it sees the host wake-up signal line has been brought LOW, indicating that all characters have been read from the GainSpan node. This completes the initialization process. At this point, the host MCU can send ‘AT’ commands to the GainSpan node. MCU should not issue a reset using the ext_reset_n signal until this initialization process is completed.
3. In case of SDIO interface, during boot up host MCU shall send dummy ‘AT’ command and wait for response from the S2W node. The host MCU must continuously send these dummy ‘AT’ commands till ‘OK’ response is received from S2W node.
4. If for some reason host MCU getting reset, then S2W adapter must be explicitly reset using EXT_RESET pin and the MCU should wait for the host wake-up signal become high in case of SPI interface. However if reset provision is not available, then host MCU must continuously send dummy ‘AT’ commands till ‘OK’ response is received from S2W adapter.



NOTE: *The SPI Host WAKE PIN for GS2011M is GPIO37.*

3.4 UART Interface Configuration

3.4.1 UART Parameters

This command is used to set the UART parameters. The UART parameters take effect immediately. However, they are stored in RAM and will be lost when power is lost unless they are saved to a profile using AT&W (see [3.9.1 Save Profile, page 87](#)). The profile used in that command must also be set as the power-on profile using AT&Y (see [3.9.3 Selection of Default Profile, page 89](#)).

Command Syntax

ATB=<baudrate>[[, <bitsperchar>] [, <parity>] [, <stopbits>]]

Usage



NOTE: All standard baud rates are supported.

Parameter Description

[Table 23, page 65](#) describes the UART interface parameters.

Table 23 **UART Interface Parameters**

Parameter	Optional/Mandatory	Value	Description
baudrate	Mandatory	9600 (default) 9600, 19200, 38400, 57600, 115200, 230400, 460800, and 921600	
bitsperchar	Optional	8 (default) 5, 6, 7, or 8	
parity	Optional	no parity (default) n - no parity (default) e - even parity o - odd parity	
stopbits	Optional	1 (default) 1 or 2 stop bits	

Synchronous Response

[Table 24, page 65](#) describes the synchronous responses and remarks for the UART Parameters command.

Table 24 **UART Parameters Responses**

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Other than the allowed baud rates or if baud rate is not entered.

3.4.2 Software Flow Control

This command is used to enable or disable software flow control for the UART interface.

Command Syntax AT&Kn

Parameter Description

Table 25, page 66 describes the Software Flow Control parameters.

Table 25 Software Flow Control Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0 (default)	Software flow control is disabled.
		1	Software flow control is enabled.

Synchronous Response

Table 26, page 66 describes the synchronous responses and remarks for the Software Flow Control command.

Table 26 Software Flow Control Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameter is not valid. (other than 0 or 1)

3.4.3 Hardware Flow Control

This command is used to enable or disable hardware flow control for the UART interface.

Command Syntax AT&Rn

Parameter Description

Table 27, page 66 describes the Hardware Flow Control parameters.

Table 27 Hardware Flow Control Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0 (default)	Hardware flow control is disabled.
		1	Hardware flow control is enabled.

Synchronous Response

Table 28, page 67 describes the synchronous responses and remarks for the Hardware Flow Control command.

Table 28 Hardware Flow Control Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameter is not valid. (other than 0 or 1)

3.5 SPI Interface and Configuration

For higher throughput application, we make use of SPI interface between MCU and GS module.

SPI mode is a combination of clock polarity and clock phase with respect to the data. There are four types of SPI modes:

- [SPI Mode 0](#)
- [SPI Mode 1](#)
- [SPI Mode 2](#)
- [SPI Mode 3](#)

For SPI Mode 0 and SPI Mode 2, the SPI Master should toggle Chip Select (CS) or Slave Select (SS) for every byte.

For SPI Mode 1 and SPI Mode 3, the SPI Master should not toggle Chip Select (CS) or Slave Select (SS) for every byte; but should be toggled for every byte stream.

The following command is used to set the SPI clock polarity and clock phase parameters. The new SPI parameters take effect after node reset/restart. However, they are stored in RAM and will be lost when power is lost unless they are saved to a profile using AT&W (see [3.9.1 Save Profile, page 87](#)). The profile used in that command must also be set as the power-on profile using AT&Y (see [3.9.3 Selection of Default Profile, page 89](#)).

Command Syntax

AT+SPICONF=<clockpolarity>,<clockphase>

Parameter Description

[Table 29, page 68](#) describes the SPI Interface Configuration parameters.

Table 29 SPI Interface Configuration Parameters

Parameter	Optional/Mandatory	Value	Description
clockpolarity	Mandatory	0 (default)	Inactive state of serial clock is low.
		1	Inactive state of serial clock is high.
clockphase	Mandatory	0 (default)	Data is captured on the first edge of the serial clock (clock phase zero), after the falling edge of slave select signal.
		1	Data is captured on the second edge of the serial clock (clock phase 180), after the falling edge of slave select signal.

Table 30, page 69 describes the configuration for clock polarity and clock phase with respect to SPI Mode.

Table 30 SPI Modes, Clock Polarity, and Clock Phase

SPI Mode	Clock Polarity	Clock Phase
0	0	0
1	0	1
2	1	0
3	1	1

Synchronous Response

Table 31, page 69 describes the synchronous responses and remarks for the SPI Interface Configuration command.

Table 31 SPI Interface Configuration Synchronous Responses

Responses	Remarks
OK	Success

3.6 SPI Interface Handling

In the case of SPI interface, the GS2011M node acts as slave and will communicate to master SPI controller. By default, SPI interface supports Motorola protocol with clock polarity 0 and clock phase 0 (default mode 0). For more detailed specification of SPI frame format and timing characteristics refer to the *Data Sheet*.

GS2000 uses two types of SPI methods to communicate with MCU:

- [SPI byte stuffing method](#)
- [SPI DMA command response method](#)

3.6.1 SPI Byte Stuffing Method

In this method, data is transferred byte by byte between the GS module and MCU. Since SPI data transfer works in full duplex mode, its required to make use of special octet to indicate idle data. Similarly, if host MCU is sending data at higher rate flow control mechanism is required. In order differentiate these special control codes (such as idle pattern, flow control codes and other control octets) from user data, byte stuffing mechanism is incorporated.

SPI transmit data handling procedure:

The SPI data transfer layer makes use of an octet (or byte) stuffing procedure. The Control Escape octet is defined as binary 11111011 (hexadecimal **0xFB**), most significant bit first. Each special control pattern is replaced by a two octet sequences consisting of the Control

Escape octet followed by the original octet exclusive-or'd (XOR) with hexadecimal **0x20**. Receiving implementations must correctly process all Control Escape sequences (Ctrl+ESC key). Escaped data is transmitted on the link as described in [Table 32, page 70](#).

Table 32 SPI Transmit Data Handling Link Pattern

Pattern	Encoded as	Description
0xFD	0xFB 0xDD	Flow control XON
0xFA	0xFB 0xDA	Flow control XOFF
0x00	0xFB 0x20	Inactive link detection
0xFB	0xFB 0xDB	Control ESCAPE
0xF5	0xFB 0xD5	IDLE character
0xFF	0xFB 0xDF	Inactive link detection
0xF3	0xFB 0xD3	SPI link ready indication

One dedicated GPIO signal (**GS_SPI_HOST_WAKEUP**) is available for data ready indications from Slave GS2000 based modules node to Master Host controller. This **GS_SPI_HOST_WAKEUP** signal is asserted high during valid data transmission period, so that the host (master SPI) starts pulling out data by giving SPI clock and **GS_SPI_HOST_WAKEUP** signal is de-asserted once transmission is completed. Master host controller must provide clock as long as **GS_SPI_HOST_WAKEUP** signal is active.

Special character (**GS_SPI_IDLE**) will be transmitted during idle period (if there is no more data to transmit) and must be dropped at the receiving Host.

SPI receive data handling procedure:

Since byte stuffing is used, each Control Escape octet must be removed and the next immediate octet is exclusive-or'd (XOR) with hexadecimal **0x20**. If received buffer has reached the upper water mark, then **XOFF** character will be sent out informing the host to stop transmitting actual data. After receiving **XOFF** character host must stop transmitting actual data and can send IDLE bytes, until the XON is received. Once the host receives **XON**, then it may resume the valid data transmissions.

Special control byte **IDLE** will be dropped at receiver.

3.6.2 SPI DMA Command Response Method

This method is used to achieve high throughput over SPI by using:

- Higher clock rate up to 10Mhz (when running @120Mhz)
- DMA access for the data transfer

This interface uses command response handling between GS2011M (always slave) and any MCU (always master which controls the clock) through SPI interface. MCU issues commands for read/write and waits for the response.

If the response indicates:

- Success: the action is taken
- Failure: the action is deferred and retried after some time or dropped.

Operation sequence: Command > Response > Data phase (if response success) > Command > Response > Data phase (response success).

The HI Format is used for the message exchange. Refer to [3.6.2.3 Annexure - HI Frame Format \(From Host Side\), page 80](#) and [3.6.2.4 Annexure - HI Frame Response \(From GS2011M Side\), page 82](#).

Based on MCU capabilities (such as multi threaded application, single threaded application, interrupt supported application, and so on), SPI command response method supports the following methodologies to transfer data between MCU and GS2000.

- [Polling methodology](#)
- [Interrupt based methodology](#)

3.6.2.1 Polling Methodology

This methodology is used when the MCU application is single threaded and cannot support interrupts.

The following section provides steps involved while transferring data from MCU to GS2000 using Polling methodology.

Transferring Data from MCU to the GS2000

1. MCU provides clock.
2. MCU sends the WRITE_REQUEST to GS2000. It uses HI frame with:
 - a. Class field - WRITE_REQUEST
 - b. Length is the size of data to be transferred from MCU to GS2000
 - The maximum data length allowed would be 2032 (2048-8-8).
 - The maximum DMA size allowed on GS2000 is 1024.
 - An allowance of 8 bytes for the header of HI frame carrying the data, and 8 bytes for the Write response HI frame is provided.
3. When the WRITE_REQUEST is received, GS2000 checks whether GPIO37 is HIGH. If it is HIGH, then GS2000 pulls down the Ready to Send Signal (GPIO37) to low. This is to avoid a race condition when the GS2000 wants to send data to MCU and MCU wants to send data to GS2000 simultaneously.



NOTE:

If a race condition occurs when the GS2000 wants to send data to MCU and MCU wants to send data to GS2000 at the same time, then:

- a.) GS2000 first responds to the WRITE_REQUEST and provides proper responses.
- b.) Once MCU WRITE is finished and MCU receives proper response, GPIO37 will be again made HIGH as GS2000 has some pending data which MCU has not read.
- c.) MCU then issues READ_REQUEST and reads out the data present in GS2000.

-
4. GS2000 pulls the Ready to Send signal (GPIO37) high to inform the MCU when it is ready with the WRITE_RESPONSE.



NOTE: The MCU must wait for the GPIO37 transition from Low to High before applying the clock. If there is pending data to be transferred from GS2000 to MCU, then GS2000 will indicate the same in the additional information field of the response which is processed by MCU.

-
5. MCU provides the clock to read WRITE_RESPONSE.
 6. GS2000 sends WRITE_RESPONSE to MCU. It uses HI frame with:
 - a. Class field – WRITE_RESPONSE
 - b. Length as the size of the data the GS2000 will be able to receive. This is 0 if GS2000 is unable to receive (flow control)
 - c. The status field is WRITE_OK if it is ready to receive the data and WRITE_NOT_OK if it is not ready to receive the data



NOTE: When GS module sends WRITE_NOT_OK to MCU, MCU should wait for a certain time (Ex: 100 msec) and then re-issue the WRITE_REQUEST. In this case, MCU should ensure that it does not drop any data.

-
- d. When the WRITE_RESPONSE is sent, GS2000 triggers an interrupt to pull down the Ready to Send Signal (GPIO low)
 7. MCU sends the data and the data header using HI Frame with:
 - a. Class field – DATA_FROM_HOST
 - b. Length as the size of the data (this length must be less than or equal to the length mentioned in the WRITE_RESPONSE)
 8. Once the entire process of WRITE is complete, MCU checks the GPIO37 for any pending data from GS2000 and GPIO is:
 - a. LOW, will stop the clock

- b. HIGH, will start the procedure for READ once it is ready to receive

The following section provides steps involved while transferring data from GS2000 to MCU using Polling methodology.

Transferring Data from the GS2000 to the MCU

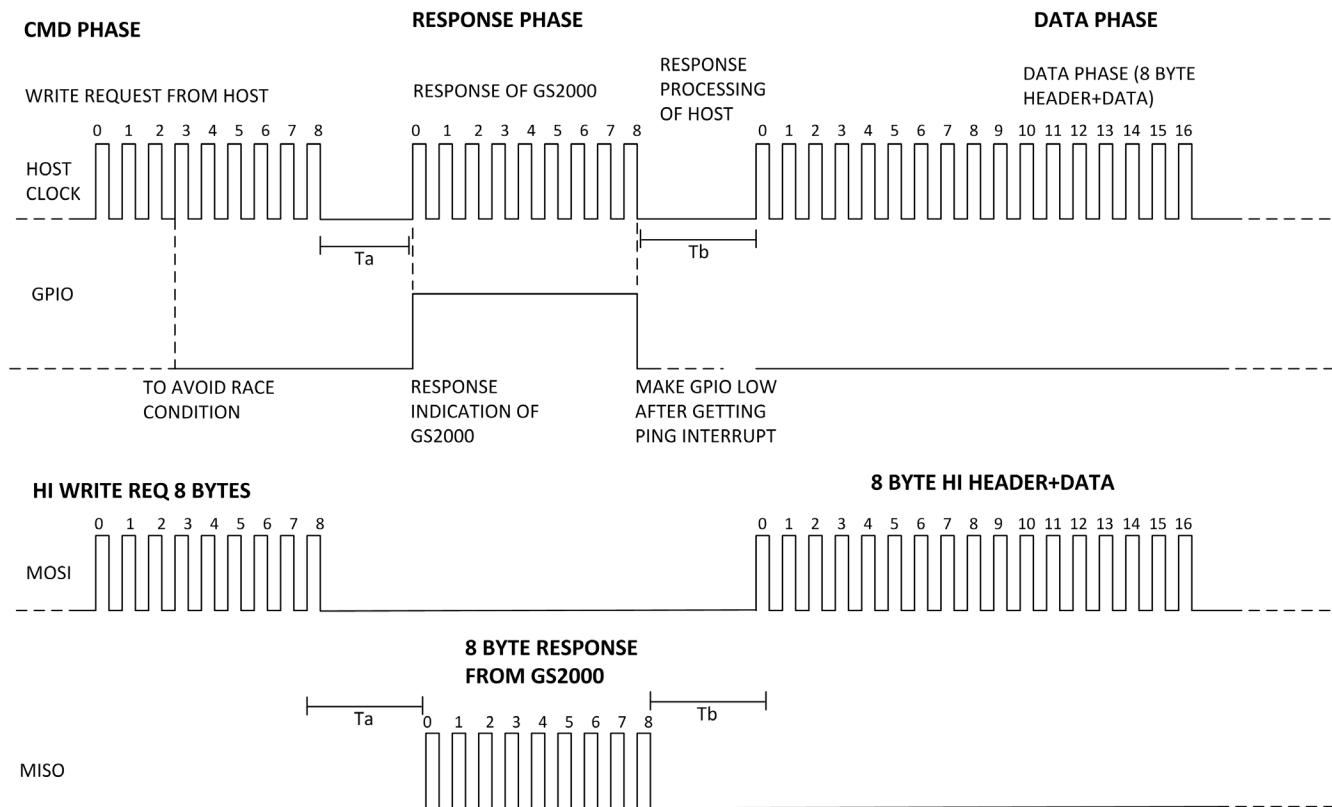
1. GS2000 pulls up the Ready to Send Signal (GPIO37) high when there is data to send from GS2000 to MCU.
2. MCU provides clock when it is willing to receive.
3. MCU sends the command READ_REQUEST to GS2000. It uses HI frame with:
 - a. Class field - READ_REQUEST
 - b. Length is the size of data that MCU is willing to receive from GS2000
 - The maximum data length allowed would be 2032 (2048-8-8).
 - The maximum DMA size allowed on GS2000 is 1024.
 - An allowance of 8 bytes for the header of HI frame carrying the data, and 8 bytes for the Write response HI frame is provided.
4. When the READ_REQUEST is received, the GS2000 triggers an interrupt to pull down the Ready to Send Signal (GPIO37) low.
5. GS2000 pulls the Ready to Send signal (GPIO37) high to inform the MCU when it is ready with the response.
6. MCU provides the clock for reading READ_RESPONSE.
7. GS2000 sends a response to the MCU. It uses HI frame with:
 - a. Class field – READ_RESPONSE
 - b. Length is the size of the data the GS2000 will be transmitting
 - c. The status field is READ_OK if it is ready to receive the data and READ_NOT_OK if it is not ready to receive the data
 - d. When the READ_RESPONSE is sent, the GS2000 will trigger an interrupt to pull down Ready to Send Signal (GPIO low)
8. GS2000 sends the data and the data header using HI Frame with:
 - a. Class field – DATA
 - b. Length is the size of the data (this length must be less than or equal to the length mentioned in the READ_RESPONSE)
9. MCU stops the clock.

Timing Diagrams

MCU Write When GS2011M Has No Data to Send

Figure 12, page 74 shows the timing diagram for MCU write when GS2011M has no data to send.

Figure 12 MCU Write When GS2011M Has No Data to Send



MCU Write When the GS2000 Has Data to Send

Figure 13, page 75 shows the timing diagram for MCU write when GS2000 has data to send.

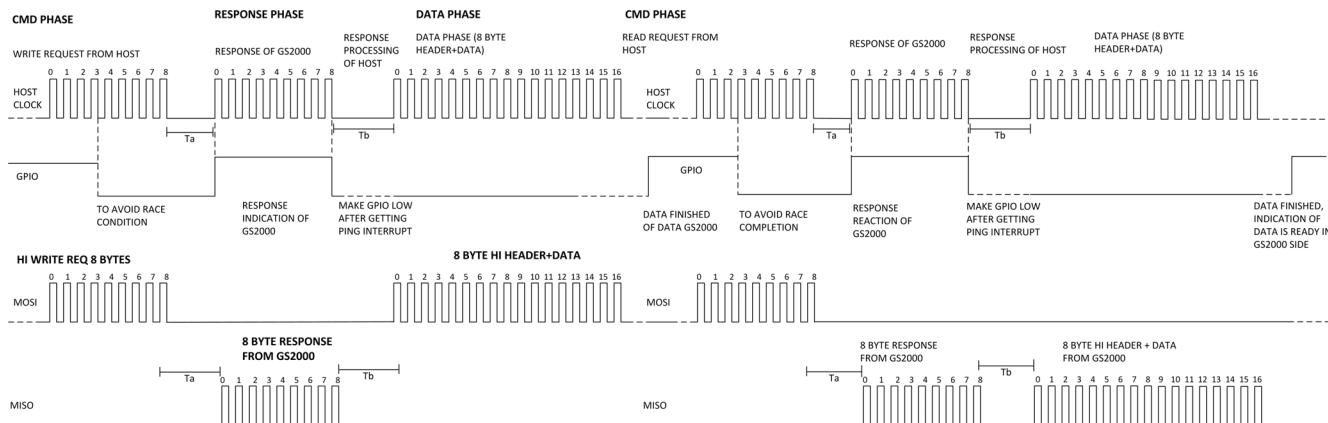
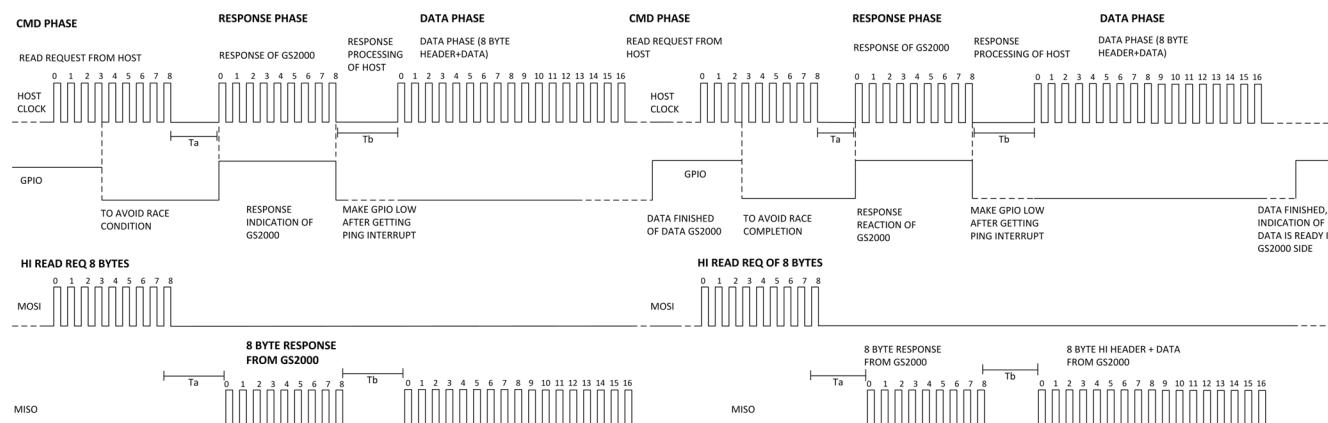
Figure 13 MCU Write When GS2000 Has Data to Send**GS Module Data Send**

Figure 14, page 75 shows the timing diagram for the GS2011M data send.

Figure 14 GS2011M Data Send

3.6.2.2 Interrupt Based Methodology

This methodology is used if the MCU is running at higher clock speed and run into false detection of GPIO37 status.

The following section provides steps involved while transferring data from MCU to GS module using Interrupt based methodology.

Transferring Data from MCU to GS module

1. MCU sends first four bytes of WRITE REQUEST to GS2000. It waits for minimum of 3.2 microseconds and rearms the interrupt handler which discards all the previous interrupts.



NOTE: When GS module sends WRITE_NOT_OK to MCU, MCU should wait for a certain time (Ex: 100 msec) and then re-issue the WRITE_REQUEST. In this case, MCU should ensure that it does not drop any data.

2. GS module receives four bytes of WRITE REQUEST in SPI FIFO. It triggers an interrupt to pull the GPIO37 low (This step is performed although GPIO37 is low).



NOTE: 1.) The MCU waits for 3.2 microseconds as it is the minimum time required for the hardware and software latency. The following steps describe how an interrupt is processed:

- a.) SPI FIFO triggers an interrupt as soon as it receives the first four bytes of data from MCU
- b.) Interrupt is sent to the interrupt controller
- c.) Interrupt controller intimates the APP CPU about the interrupt
- d.) OS scheduler checks for any pending interrupt and runs the corresponding ISR (Interrupt Service Routine) as ISRs have the highest priority

**NOTE:**

2.) If a race condition occurs when the GS module wants to send data to MCU and MCU wants to send data to GS module at the same time, then this scenario is being handled as follows:

When data is received over the network which is supposed to be sent to MCU, the task that is responsible for making the GPIO37 high can never run ahead of the ISR even though the interrupts are disabled in the system.

Disabling of interrupts is being done by tasks who have a higher priority than the application receive task which makes the GPIO37 high when there is data to be sent to MCU.

While the interrupts are disabled, a thread switch can only happen if there is:

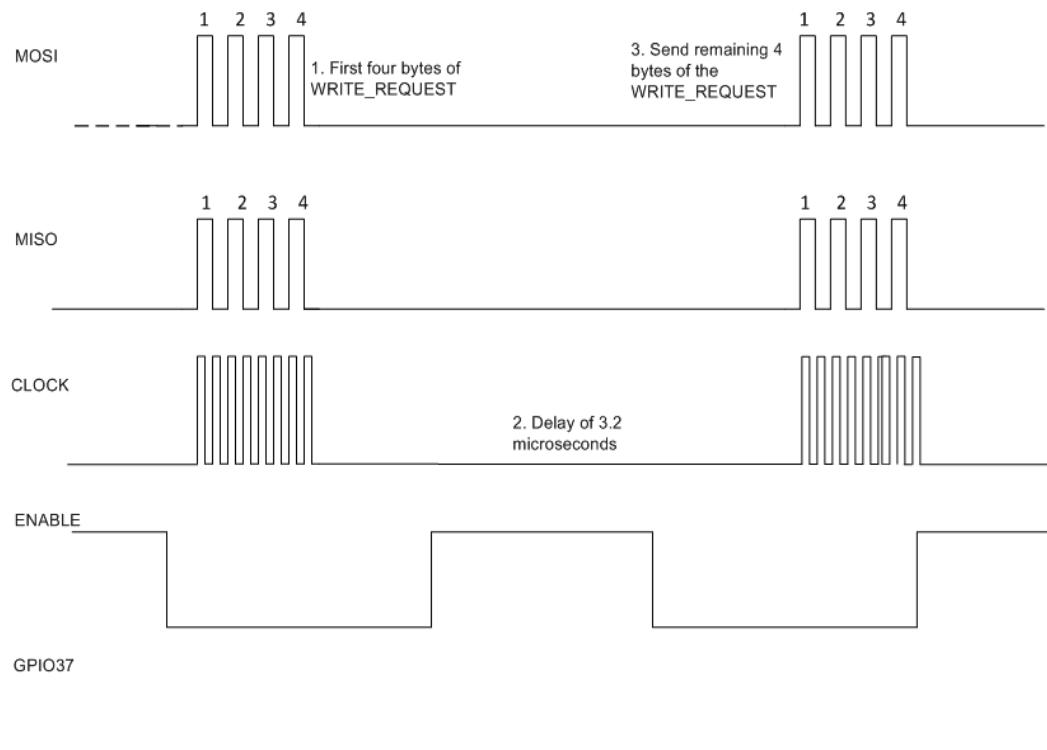
- a message post to a higher priority thread or*
- semaphore acquire/release happening or*
- any RTOS call that can make thread switch even before the interrupts are enabled.*

And in no circumstances, this is happening in our system which avoids the mentioned race condition.

3. MCU sends the remaining four bytes of the WRITE REQUEST and waits for the GPIO37 to transit from low to high.

Figure 15, page 78 shows the timing diagram from step 1 to step 3.

Figure 15 Transferring data from MCU to GS Module



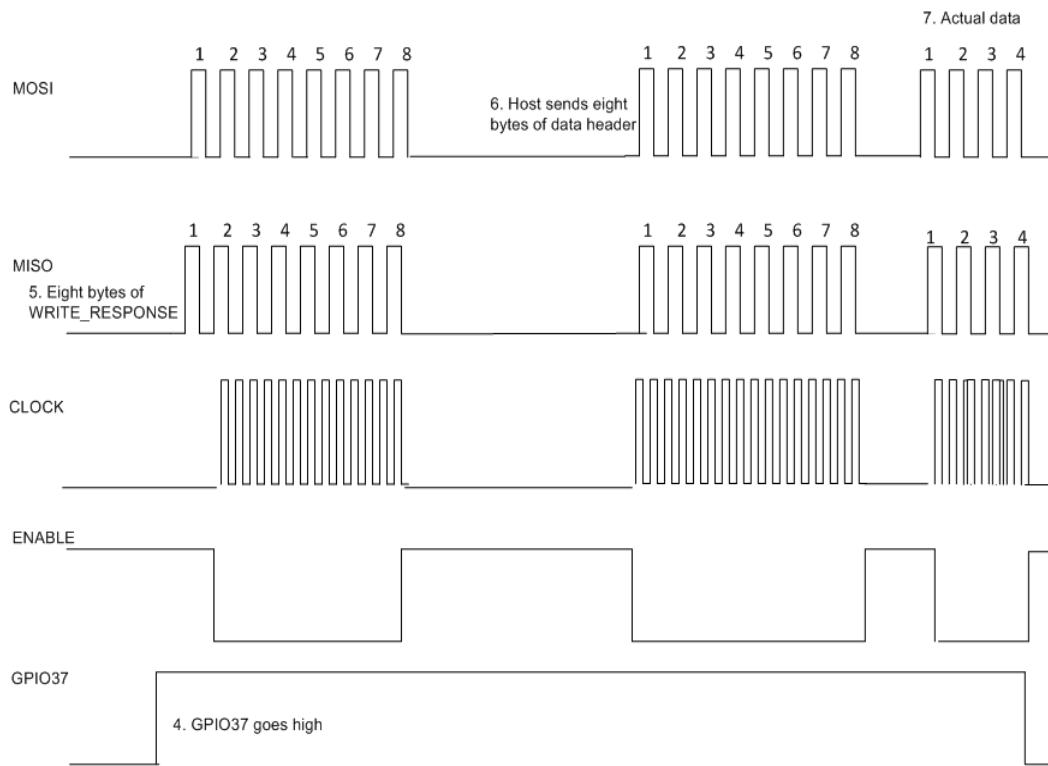
4. GS module receives the four bytes in SPI FIFO. It parses the WRITE REQUEST and formulates the WRITE RESPONSE.
5. GS module puts the eight bytes of WRITE RESPONSE in Ping buffer and pulls the GPIO37 high.
6. MCU detects the GPIO37 as high and sends clock to receive the WRITE RESPONSE.
7. MCU parses the WRITE RESPONSE, learns the amount of data that can be received by GS module, and provides eight bytes of Data header to GS module.



NOTE: When the size of data is less than 1024 bytes, the time GPIO37 takes to become low after step 5 is 16 clock cycles (READ RESPONSE + Data Header). When the size of data is more than 1024 bytes, the wait cycle will be (Data length-1024+16) clocks. This is because the PONG Tx buffer is of 1024 bytes in size and the initial extra bytes (Data length - 1024) are put in PING Tx buffer.

8. MCU sends the actual data.

Figure 16, page 79 shows the timing diagram from step 4 to step 8.

Figure 16 Transferring data from MCU to GS Module (Contd.)

The following section provides steps involved while transferring data from GS module to MCU using Interrupt based methodology

Transferring Data from GS Module to MCU

1. When GS module has data to be sent to MCU, it makes the GPIO37 high.
2. On receiving an interrupt, MCU performs the following:
 - a. Rearms the interrupt handler to detect the low to high transition of GPIO37
 - b. Sends eight bytes of READ REQUEST to GS module
 - c. Waits for the low to high transition of GPIO37
3. GS module receives the eight bytes of READ REQUEST and triggers an interrupt to pull the GPIO37 low.
4. GS module parses the READ REQUEST, formulates the READ RESPONSE, puts the READ RESPONSE along with the Data header in the PING buffer, and pulls the GPIO37 high.
5. MCU detects the GPIO37 as high and sends clock to receive the READ RESPONSE.
6. MCU parses the READ RESPONSE, learns the amount of data that will be sent by GS module, and provides clock to receive eight bytes of Data header and actual data.

Points to Remember

Points to remember from MCU perspective when using Interrupt based methodology:

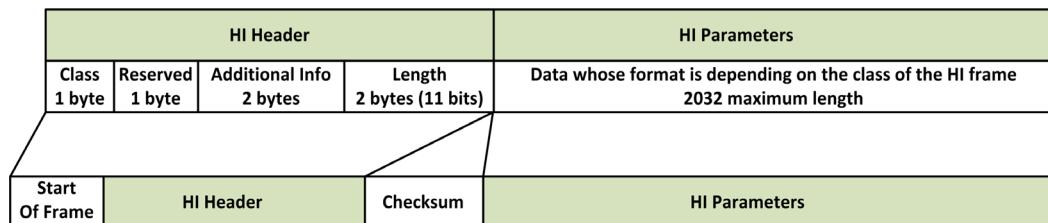
- GS module performs an automatic soft-reset if pending network data has not been received by the MCU for 32 seconds.
- MCU is not allowed to abort a read/write operation after issuing a READ_REQUEST or WRITE_REQUEST.
- The data length value in the DATA_HEADER should always be identical to the data length value in the respective READ_RESPONSE or WRITE_RESPONSE.
- GS module never uses a data length value of 0 bytes in READ_RESPONSE or WRITE_RESPONSE, and DATA_HEADER. GS module sends NOK If there is no data to read or write.
- MCU should never use a data length value of 0 bytes in DATA_HEADER.
- GS module does not expect any inter-word time between the transmissions of SPI words to receive data. This means, when clock is given by the MCU, the GS module sends data that is available in its SPI buffer and when the clock is stopped, this data stays in the SPI buffer.
- Idle characters are represented by 0xF5.

3.6.2.3 Annexure - HI Frame Format (From Host Side)

All messages carried over the Host Interface have a common format. They are composed of a HI header, and parameters depending on the header. HI frames are composed, in addition to the HI header and parameters, of a start delimiter and a HI HEADER checksum. This format is defined in [Figure 17, page 80](#) below.

The Start-of-frame delimiter is the single-byte value 0xA5, used to ensure synchronization at the frame level. The driver starts the reception process when it recognizes the delimiter. The length of the delimiter has been reduced to 1 byte to avoid alignment problems when waiting for the start element. However, no provisions are made to ensure that the subsequent data stream does not contain a byte with value 0xA5, so it is possible for the driver to mistake a data byte for a delimiter. Therefore, a header checksum has been added to ensure correct synchronization. A single checksum byte is used, computed as the 1's complement of the 8-bit long (modulo-256) sum of all the bytes of the HI HEADER (not including the Start delimiter). Note that each byte is independently added to the sum, as an integer between 0 and 255, without regard for its significance within its own data field.

Figure 17 HI Frame Format (From Host Side)



The format of HI Parameters field is determined by the service class. The service class of each frame is signaled by the value of the first field. Available service class identifiers (see Table 33, page 81).

Table 33 HI Parameters Service Class Identifiers

Identifiers	Description
Start of frame	0xA5
Class	0x01 - WRITE_REQUEST from MCU side 0x02 - READ_REQUEST from MCU side 0x04 - READWRITE_REQUEST from MCU side 0x03 - DATA from MCU side
Reserved	0x00
Additional Info	0x00,0x00
Length	Maximum 2032
CheckSum	A single checksum byte is used, computed as the 1's complement of the 8-bit long (modulo-256) sum of all the bytes of the HI HEADER (not including the Start delimiter).

3.6.2.4 Annexure - HI Frame Response (From GS2011M Side)

Figure 18, page 82 shows the HI Frame Response from the GS2011M side.

Figure 18 HI Frame Response (from GS2011M Side)

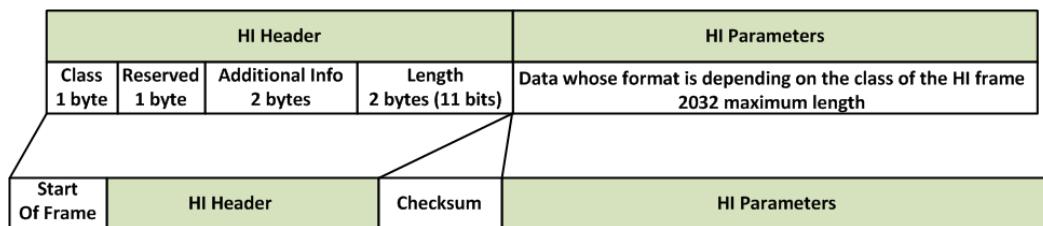


Table 34, page 82 shows the HI Frame Response from the GS2011M side.

Table 34 HI Frame Response (from GS2011M Side)

Identifier	Description
Start of frame	0xA5
Class	0x11 - WRITE_RESPONSE_OK to MCU side 0x12 - READ_RESPONSE_OK to MCU side 0x13 - WRITE_RESPONSE_NOK to MCU side 0x14 - READ_RESPONSE_NOK to MCU side 0x16 - READWRITE_RESPONSE_OK to MCU side 0x17 - READWRITE_RESPONSE_NOK to MCU side. 0x15 - DATA to MCU side
Reserved	0x00
Additional Info	0x00,0x00 0x00, 0x01 - Pending Data for transfer from GS2000 to MCU
Length	0 (No Data)
CheckSum	A single checksum byte is used, computed as the 1's complement of the 8-bit long (modulo-256) sum of all the bytes of the HI HEADER (not including the Start delimiter).

3.6.2.5 Pin Connection for SPI Interface

Table 35, page 83 describes the pin connection for the SPI interface.

Table 35 Pin Connection for SPI Interface

Host MCU	S2W Node	Remarks
MSPI_DOUT	SSPI_DIN	N/A
MSPI_DIN	SSPI_DOUT	N/A
MSPI_SS	SSPI_SS	N/A
MSPI_CLK	SSPI_CLK	N/A
GPIO	GPIO37	Host wake-up signal or Ready to Send.
Ground	Ground	Ground

3.6.3 SDIO Interface

The Serial-to-WiFi (S2W) adapter supports SDIO interface with a maximum clock frequency of up to 33MHz. The data bus width can be either 1 bit or 4 bit mode. There is no command available to configure the SDIO interface.

3.7 Serial-to-WiFi Configuration

This command is used to help configure various MAC layer and network layer configurations. *n* is the parameter id to set and *p* is the value to set the parameter to.

Command Syntax ATSn=p

Parameter Description

Table 36, page 84 describes the Serial-to-WiFi Configuration parameters.

Table 36 Serial-to-WiFi Configuration Parameters

Parameter	Name	Value	Description
2	CommandMode-TCP Connection Timeout (for Transport layer or TCP/UDP connection)	500 i.e., $500 \times 10 = 5000$ ms (5 seconds) (default)	The maximum amount of time allowed establishing a TCP client connection, in units of 10 milliseconds. Allowed values: 1 to 65535 (but the TCP/IP stack limits the maximum timeout value).
3	Association Retry Count	N/A	Not currently supported.
4	AutoMode-Nagle Wait Time	10, i.e., $10 \times 10 = 100$ ms (default)	The data which the GS node receives from the MCU will buffer up to this (AutoMode-Nagle Wait Time) or the amount of data is limited by available buffer size (i.e., 1400 bytes). That means if it is any one of these becomes true then that data will be sent over serial interface in units of 10 milliseconds. Allowed values: 1 to 65535 (but the amount of data is limited by available buffer size, i.e., 1400 bytes).
5	CommandMode-Scan Time (Ob	150 (150 ms) (default)	The maximum time for scanning in one radio channel, in units of milliseconds. This command is deprecated by the new command AT+WST (see 3.10.5 Set Scan Time, page 96). Allowed values: 5 to 1200 (but at the high limit a 14-channel scan will consume 4 minutes).

Table 36 Serial-to-WiFi Configuration Parameters (Continued)

Parameter	Name	Value	Description
6	NcmAutoMode-Transport Layer-Retry Period	50 (50x10=500 msec) (default)	The time in period between each transport layer 4 connection retry with Ncm auto in units of 10 milliseconds.
7	NcmAutoMode-Transport Layer Retry Count	20 (default)	<p>It is the number of TCP connection retries in NCM auto mode.</p> <p>The node sends the first TCP connection request.</p> <p>If the connection is successful, then the node receives CID.</p> <p>If the connection is not successful, then it starts the timer (NcmAutoMode-Transport Layer-Retry Period), waits for it to expire, and then sends the second TCP connection request.</p> <p>Note: To achieve infinite retries in NCM auto mode, set the retry count to 4294967295.</p>
8	Auto connection exit sequence (+++) enabled timeout	1	<p>The time to wait to come out of auto mode after the auto connection exit sequence (+++) enabled timeout.</p> <p>The default value for this parameter is 100 milliseconds (1 second).</p> <p>The maximum value for this parameter is 1000 milliseconds (10 seconds).</p> <p>This feature can be disabled by setting the parameter value to 0.</p>

Synchronous Response

Table 37, page 85 describes the synchronous responses and remarks for the Serial-to-WiFi Configuration command.

Table 37 Serial-to-WiFi Configuration Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.8 Identification Information

This command is used to return various adapter identification information.

Command Syntax ATIn

Parameter Description

Table 38, page 86 describes the Identification Information parameters.

Table 38 Identification Information Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0	OEM identification
		1	Hardware version
		2	Software version
<i>n</i> is the information ID to obtain. These responses are provided as ASCII strings in addition to the standard command response.			

Synchronous Response

Table 39, page 86 describes the synchronous responses and remarks for the Identification Information command.

Table 39 Identification Information Synchronous Responses

Responses	Remarks
GainSpan OK	Success
ATI1:GSxxxx OK	The hardware version will change whenever the code in the ROM gets changed.
ATI2:x.x.x OK	The software version will change whenever a new feature is added.
ERROR:INVALID INPUT	If parameters are not valid. (<i>n</i> value is other than 0-2)

3.9 Serial-to-WiFi Profile Configuration

The GS node configuration parameters can be stored in a profile. These profiles are stored in non-volatile memory. See [2.1.2 Profile Definition, page 33](#) for a detailed description of the profile parameters.

3.9.1 Save Profile

This command is used to save the current profile. Upon deployment of this command, the current configuration settings are stored in non-volatile memory under the specified profile, (profile 0, or profile 1). In order to ensure that these parameters are restored after power cycling the GS node, the command AT&Y must also be issued, using the same profile number selected here.

Command Syntax AT&Wn

Parameter Description

[Table 40, page 87](#) describes the Save Profile parameters.

Table 40 Save Profile Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0	For profile 0
		1	For profile 1
	Saves the profile specified by n (0 or 1).		

Synchronous Response

[Table 41, page 87](#) describes the synchronous responses and remarks for the Save Profile command.

Table 41 Save Profile Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid. (n value is other than 0 or 1)



NOTE: The GS2011M supports two profiles.

3.9.2 Load Profile

This command is used to load a profile. Upon deployment of this command, the currently configured settings are overwritten by those stored in non-volatile memory under the specified profile

Command Syntax ATZn

Parameter Description

Table 42, page 88 describes the Load Profile parameters.

Table 42 Load Profile Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0	For profile 0
		1	For profile 1
	Load the profile specified by n (0 or 1).		

Synchronous Response

Table 43, page 88 describes the synchronous responses and remarks for the Load Profile command.

Table 43 Load Profile Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid. (n value is other than 0 or 1)

3.9.3 Selection of Default Profile

This command is used to select the default profile. The settings from the profile that are chosen as the default profile are loaded from non-volatile memory when the device is started.

Command Syntax AT&Yn

Parameter Description

Table 44, page 89 describes the Selection of Default Profile parameters.

Table 44 Selection of Default Profile Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0	For profile 0
		1	For profile 1
			Set default profile to the value n (0 or 1).

Synchronous Response

Table 45, page 89 describes the synchronous responses and remarks for the Selection of Default Profile command.

Table 45 Selection of Default Profile Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid. (n value is other than 0 or 1)

Example AT&Y0
OK



NOTE: The GS2011M supports two profiles.

3.9.4 Restore to Factory Defaults

This command is used to restore current profile to factory default values. The factory default values are stored in RAM, and will be lost after each power cycle.

Upon deployment of this command, the current configuration variables are reset to the factory defaults. These defaults are defined by macro values in the configuration header. Issuing this command resets essentially all configuration variables.

Command Syntax AT&F

Synchronous Response

[Table 46, page 90](#) describes the synchronous responses and remarks for the Restore to Factory Defaults command.

Table 46 Restore to Factory Defaults Synchronous Responses

Responses	Remarks
OK	Success

3.9.5 Output Current Configuration

This command is used to output the configuration of current and saved profile parameter values in ASCII. The details of the profile parameters are described in [2.1.2 Profile Definition, page 33](#).

Command Syntax AT&V

Synchronous Response

[Table 47, page 91](#) describes the synchronous responses and remarks for the Output Current Configuration command.

Table 47 Output Current Configuration Synchronous Responses

Responses	Remarks
ACTIVE PROFILE C0 &Y0 E1 V1 B=9600,8,N,1 &K0 &R0 +NDHCP=0 +NSET=192.168.1.99,255.255.255.0,192.168.1.1 +DNS1=0.0.0.0, +DNS2=0.0.0.0 +WM=0 +WAUTO=0,"GSDemoKit",,6 +WRETRY=5 +WP=0 +WRXPS=1 +WRXACTIVE=0 +N AUTO=0,1,192.168.1.1,8 +W AUTH=0 +WWPA="Serial2Wifi"+PSK-valid=0 +SSID= +WEPP1=1234567890 +WEPP2= +WEPP3= +WEPP4= S0=01000 S1=00500 S2=00500 S3=00003 S4=00010 S5=00150 S6=00050 S7=00020 S8=01400 +B DATA=0 +WSEC=0 +ASYNCMSG=0	Success The number of profiles depends upon the default configuration of the module.
STORED PROFILE 0 E1 V1 B=9600,8,N,1 &K0 &R0 +NDHCP=0 +NSET=192.168.1.99,255.255.255.0,192.168.1.1 +DNS1=0.0.0.0, +DNS2=0.0.0.0 +WM=0 +WAUTO=0,"GSDemoKit",,6 +WRETRY=5 +WP=0 +WRXPS=1 +WRXACTIVE=0 +N AUTO=0,1,192.168.1.1,8 +W AUTH=0 +WWPA="Serial2Wifi"+PSK-valid=0 +SSID= +WEPP1=1234567890 +WEPP2= +WEPP3= +WEPP4= S0=01000 S1=00500 S2=00500 S3=00003 S4=00010 S5=00150 S6=00050 S7=00020 S8=01400 +B DATA=0 +WSEC=0 +ASYNCMSG=0 OK	Success

3.10 WiFi Interface Configuration

3.10.1 Set MAC Address

This command is used to set the MAC address to the GS node.

The MAC address is used in the 802.11 protocol to identify the various nodes communicating with an Access Point and to route messages within the local area (layer 2) network. Fixed MAC addresses issued to network interfaces are hierarchically structured and are intended to be globally unique. Before issuing a MAC address to a given Adapter, ensure that no other local device is using that address.

Command Syntax AT+NMAC=<MAC ADDRESS>

Parameter Description

Table 48, page 92 describes the Selection of Set MAC Address parameters.

Table 48 Set MAC Address Parameters

Parameter	Optional/Mandatory	Value	Description
MAC Address	Mandatory	xx:xx:xx:xx:xx:xx (17 characters)	The format of the MAC address is a 17 character colon-delimited hexadecimal number. The MAC address supplied is saved to Flash memory, and will be used on each subsequent cold boot (from power Off) or warm boot (from Standby).

Synchronous Response

Table 49, page 92 describes the synchronous responses and remarks for the Set MAC Address command.

Table 49 Set MAC Address Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If value is not in the valid format.

Example

AT+NMAC=00:1d:c9:d0:70:cc
OK

AT+NMAC=?
00:1d:c9:d0:70:cc
OK

3.10.2 Get MAC Address

This command is used to output the current MAC address of the wireless interface to the serial port.

Command Syntax AT+NMAC=?

Synchronous Response

Table 50, page 93 describes the synchronous responses and remarks for the Get MAC Address command.

Table 50 Get MAC Address Synchronous Responses

Responses	Remarks
OK	Success

Example AT+NMAC=?
00:1d:c9:d0:70:cc
OK

3.10.3 Set Regulatory Domain

This command is used to configure the adapter parameters to the requested regulatory domain.

Command Syntax

AT+WREGDOMAIN=<Regulartory Domain>



NOTE: We recommend setting the regulatory domain using SDK builder. If it is not set using SDK builder or if it needs to be changed, then this should be the first command issued after the Serial-to-WiFi prompt. This will automatically save the information in the profile.

Parameter Description

Table 51, page 94 describes the Set Regulatory Domain parameters.

Table 51 Set Regulatory Domain Parameters

Parameter	Optional/ Mandatory	Value	Regulatory Domain	Supported Channels	Desired Power Level
Regulatory Domain	Mandatory			Internal PA (0 as default)	External PA (2 as default)
		0 (default)	FCC	1 to 11	0-7
		1	ETSI	1 to 13	0-7
		2	TELEC	1 to 14	0-7
		The Regulatory domain set is required only once since it is being updated in the Flash.			

Synchronous Response

Table 52, page 94 describes the synchronous responses and remarks for the Set Regulatory Domain command.

Table 52 Set Regulatory Domain Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid. (If Register domain value is other than 0-3)

3.10.4 Get Regulatory Domain

This command is used to output the current regulatory domain of the wireless interface to the serial port.

Command Syntax

AT+WREGDOMAIN=?

Synchronous Response

Table 53, page 95 describes the synchronous responses and remarks for the Get Regulatory Domain command.

Table 53 Get Regulatory Domain Synchronous Responses

Responses	Remarks
REG_DOMAIN=FCC	Success
OK	

Example

AT+WREGDOMAIN=?
REG_DOMAIN=FCC
OK

Where possible values of REG_DOMAIN are: FCC, ETSI, TELEC

3.10.5 Set Scan Time

This command is used to set the minimum and maximum scan time per channel. The maximum scan time should always be greater than or equal to the minimum scan time. This command also modifies the scan time configured with the ATS5 command.



NOTE: This is the recommended method to set scan time per channel and obsoletes all other methods to configure scan time including ATS5 command. (see [3.7 Serial-to-WiFi Configuration, page 84](#)).

Command Syntax

AT+WST=<Min scan time>, <Max scan time>

Parameter Description

[Table 54, page 96](#) describes the Set Scan Time parameters.

Table 54 Set Scan Time Parameters

Parameter	Optional/Mandatory	Value (milliseconds)	Description
Min scan time	Mandatory	5-16000, 150 (default)	This is the minimum scan time per channel.
Max scan time	Mandatory	5-1200, 150 (default)	This is the maximum scan time per channel.

Synchronous Response

[Table 55, page 96](#) describes the synchronous responses and remarks for the Set Scan Time command.

Table 55 Set Scan Time Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

Example

AT+WST=150, 150
OK

3.10.6 Get Scan Time

This command is used to display minimum and maximum scan time in milliseconds.

Command Syntax AT+WST=?

Synchronous Response

Table 56, page 97 describes the synchronous responses and remarks for the Get Scan Time command.

Table 56 Get Scan Time Synchronous Responses

Responses	Remarks
	Success
MinScanTime=150	Displays “MinScanTime” and “MaxScanTime” which is configured using AT+WST command.
MaxScanTime=150	
OK	By default it displays the default values that is 150ms (milliseconds) for min and max scan time.

Example

```
AT+WST=?  
MinScanTime=150  
MaxScanTime=150
```

3.10.7 Scanning

This command is used to scan for networks with the specified parameters and displays the results. Scanning can be performed to find networks with specific SSID or in a particular operating channel, or a combination of these parameters. Scanning for a specific SSID employs active scanning, in which probe requests are transmitted with the SSID fields being filled appropriately.

Command Syntax

AT+WS [=SSID] [,BSSID] [,Channel] [,Scan Time]

Parameter Description

[Table 57, page 98](#) describes the Scanning parameters.

Table 57 Scanning Parameters

Parameter	Optional/Mandatory	Value	Description
SSID	Optional	N/A	A string containing ASCII characters between 1 and 32 (see 2.6.3 SSID and Passphrase, page 51). When SSID is specified, the GS module only scans the configured SSID.
BSSID	Optional	N/A	This command does not support scan based on the BSSID.
Channel	Optional	N/A	If channel is specified, then the node scans only that particular channel, else it scans all valid channels based on configured reg domain.
Scan Time	Optional	5-16000 (milliseconds) 150 (default)	(see 3.10.5 Set Scan Time, page 96) Configuring scan time using this parameter is obsolete. The recommended method to set scan time per channel is by using AT+WST command (see 3.10.5 Set Scan Time, page 96).

Synchronous Response

[Table 58, page 98](#) describes the synchronous responses and remarks for the Scanning command.

Table 58 Scanning Synchronous Responses

Responses	Remarks
<BSSID><SSID><Channel><Type><RSSI><Security>	Success
No. Of AP Found:<n>	Type is INFRA for infrastructure network and ADHOC for ad-hoc networks.
OK	

**Example Use Case 1 -
for Infrastructure****Network**

```
AT+WS=GainSpanDemo,,11
BSSID                      SSID          Channel Type RSSI Security
c8:d7:19:75:74:fb,        GainSpanDemo ,11, INFRA, -39, NONE
No. of AP Found:1
OK
```

**Example Use Case 2 -
for Ad-Hoc Network**

```
AT+WS=GainSpanAdHoc
BSSID                      SSID          Channel Type RSSI Security
62:67:20:01:f1:07,        GainSpanAdHoc ,11, ADHOC, -30, NONE
No. of AP Found:1
OK
```

3.10.8 Mode

This command is used to set the wireless mode and related parameters.

Command Syntax

```
AT+WM=n [, <beacon interval in AP mode>, <broadcast ssid in AP mode>,
<no. of stations allowed in AP mode>, <dtim period in AP mode>,
<inactivity timeout in AP mode>, <group key renewal interval in AP mode>]
```

Parameter Description

Table 59, page 100 describes the parameters in Mode.

Table 59 Mode Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0, 2, 5 0: WiFi station mode 2: WiFi limited AP mode 5: ISOTX	It specifies the wireless mode to be set.
beacon interval in AP mode	Optional	50 to 1500 Unit: milliseconds Default value: 100ms	It is the interval in which the node sends beacon frames.
broadcast SSID in AP mode	Optional	0, 1 0: Enable 1: Disable Default value: 0	When the mode is set to limited AP mode, this parameter specifies whether to broadcast SSID in beacon frames or not.
No. of stations in AP mode	Optional	1 - 64 Minimum value: 1 Maximum value: 64 Default value: 8	It specifies the number of stations supported in limited AP mode.

Table 59 Mode Parameters

Parameter	Optional/Mandatory	Value	Description
dtim period in AP mode	Optional	Minimum value: 1 Default value: 3	It specifies the dtim period in AP mode. For more information, refer 802.11 specification.
inactivity time-out in AP mode	Optional	2 to 65535 seconds Minimum value: 2 Default value: 360 Unit: seconds	It specifies the time-out interval when there is no activity from connected nodes. When there is no activity from a connected node, the module waits for 360 seconds and sends a probe to the inactive node. If there is no response, then it disconnects itself from the inactive node.
group key renewal interval in AP mode	Optional	Minimum value: 1 Default value: 3600 Unit: seconds	It specifies the time frame to regularly renew the group key in limited AP mode. The group key is renewed after every 3600 seconds by default.

Synchronous Response

Table 60, page 101 describes the synchronous responses and remarks for the Configure Mode command.

Table 60 Mode Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid

3.10.9 Associate with or Create an Infrastructure (AP) Network

This command is used to create or join an infrastructure network (limited access point mode).

Command Syntax

AT+WA=<SSID> [, <BSSID>] [, <Ch>], {Rssi Flag}]

•

Usage

The following is the behavior of the command in different modes:

1. In STA mode, i.e., AT+WM=0 (see [3.10.8 Mode, page 100](#)). The node will attempt to associate with the requested network. If the requested network is not available, an error message will display.
2. In AP mode, i.e., AT+WM=2 (see [3.10.8 Mode, page 100](#)), The node creates an infrastructure (Limited AP) network with the specified SSID. Issue AT+WSEC=n (refer [3.11.2 Security Configuration, page 116](#) for values) to create Limited AP with security as specified in [Table 80Security Configuration Parameters, page 116](#).

Parameter Description

Table 61, page 103 describes the associate with a Network or create an Infrastructure (AP) Network parameter.

Table 61 Associate with Network or Create an AP Network Parameters

Parameter	Optional/Mandatory	Value	Description
SSID	Mandatory	1-32 characters	The SSID is a string containing between 1 and 32 ASCII characters. See 2.6.3 SSID and Passphrase, page 51 for SSID format details.
BSSID	Optional	MAC is the 17 characters colon-delimited hexadecimal number (xx:xx:xx:xx:xx:xx)	BSSID of the Access point. In STA mode, upon this configuration the module will associate if both SSID and BSSID matches. Where as, if BSSID is not provided, module will try matching the SSID. In Limited AP mode, this shall be the same as the modules MAC address. I
Channel	Optional	Depends on the value of AT+WREGDOMAIN (see 3.10.3 Set Regulatory Domain, page 94)	In STA mode , the module will search for required SSID in that particular channel only. However, if the channel is not specified it will scan all configured networks, starting from channel number 1 to maximum allowed channels, and associate them to the first network which matches the SSID or BSSID if provided. In Limited AP mode , the module will create an access point in that particular channel. However, if the channel is not provided the module will create an access point in the channel number 1.
Rssi Flag	Optional	0: Disable 1: Enable	The module will associate to the AP with the first found SSID or BSSID based on the mentioned SSIDs or BSSIDs. The module will associate to the access point with the given SSID.

Synchronous Response

Table 62, page 104 describes the synchronous responses and remarks for associating with a network or creating an AP network.

Table 62 Associate with Network or Create an AP Network Synchronous Responses

Responses	Remarks
IP SubNet Gateway IPaddress: SubNetaddress: Gateway address	Success
ERROR:INVALID INPUT	If parameters are not valid.
ERROR	See 3.10.13 Error Code, page 109. Reissue the AT+LOGLVL command to get more details about the kind of error. Response changes based on LOGLVL.
ERROR:IP CONFIG FAIL	If DHCP fails in infrastructure mode.

Example

```
AT+WA=GainSpanDemo,,11
IP           SubNet      Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK
```

3.10.10 Disassociation

This command is used to disassociate the current infrastructure network or stop the limited AP created by the node.

Command Syntax

AT+WD

Synchronous Response

Table 63, page 104 describes the synchronous responses and remarks for the Disassociation command.

Table 63 Disassociation Synchronous Responses

Responses	Remarks
OK	Success

Asynchronous Response

Table 64, page 104 describes the asynchronous responses and remarks for the Disassociation command.

Table 64 Disassociation Asynchronous Responses

Responses	Remarks
314Dissassocation Event	AP resets or connection to the AP is lost.

Example

```
AT+WD
OK
```

3.10.11 WPS

This command is used to associate to an access point using WPS. Upon execution of this command, the GS node uses either push button or pin method or default pin method as per the METHOD parameter to associate to the WPS enabled AP.

Command Syntax

For Push Button (PBC) method:

```
AT+WWPS=<METHOD> [,PIN] [,StoreL2ConInfo] [,SSID]
```

For Pin method and Default Pin method:

```
AT+WWPS=<METHOD> [,PIN] [,SSID] [,StoreL2ConInfo]
```

Parameter Description

Table 65, page 105 describes the WPS parameters.

Table 65 WPS Parameters

Parameter	Optional/Mandatory	Value	Description
METHOD	Mandatory	1	Push Button method (PBC)
		2	Pin method
		3	Default Pin method
PIN	Optional	N/A	The pin can be any valid WPS pin (valid for pin method only). For example, 95644691.
StoreL2ConInfo	Optional	0	Disable - WiFi layer (L2) configuration parameters will not be stored in the profile.
		1	Enable - WiFi layer (L2) configuration parameters are stored in the profile.
Note: The <i>StoreL2ConInfo</i> parameter stores the WiFi layer configuration parameters which will be used during auto connection mode.			
SSID	Optional Note: It is mandatory when default PIN method (3) is used.	N/A	SSID of the AP which associates with WPS procedure.

Synchronous Response

Table 66, page 106 describes the synchronous responses and remarks for the WPS command.

Table 66 WPS Synchronous Responses

Responses	Remarks
SSID=<ssid>\r\n	
CHANNEL=<channel>\r\n	Success
OK	
ERROR:INVALID INPUT	If parameters are not valid.
ERROR	Valid parameters are provided but PBC is not started or PIN is not registered in AP. GS node will scan for 2 minutes in case of PBC and PIN methods.

Command Note

Upon success, host shall issue AT+NDHCP=1 to acquire network address (IP address) or configure the IP address statically (AT+NSET).

Example 1 - Push Button Configuration (PBC) method

```
AT+WWPS=1,,1
SSID=GainSpanDemo
CHANNEL=11
OK
```

Example 2 - PIN method

```
AT+WWPS=2,40057583,,1
SSID=GainSpanDemo
CHANNEL=11
OK
```

3.10.12 Status

This command is used to retrieve information about the current network status.

Command Syntax

AT+NSTAT=?

Synchronous Response

Table 67, page 107 describes the synchronous responses and remarks for the Status command.

Table 67 Status Synchronous Responses

Responses	Remarks
MAC=00:1d:c9:d0:70:cc WSTATE=CONNECTED MODE=AP BSSID=c8:d7:19:75:74:fb SSID="GainSpanDemo" CHANNEL=11 SECURITY=NONE RSSI=-32 IP addr=192.168.1.99 SubNet=255.255.255.0 Gateway=192.168.1.1 DNS1=0.0.0.0 DNS2=0.0.0.0 Rx Count=22 Tx Count=75090 OK	<ul style="list-style-type: none"> Success Upon deployment of this command, the adapter reports the current network configuration to the serial host: MAC address WLAN state: CONNECTED or NOT CONNECTED Mode: STA, LAP, NONE BSSID: <p>In case of STA mode, it specifies the MAC address of the connected AP.</p> <p>In case of LAP mode, it specifies the MAC address of the module itself.</p> <ul style="list-style-type: none"> SSID: <p>In case of STA mode, it specifies the SSID of the connected AP.</p> <p>In case of LAP mode, it specifies the SSID of the module itself.</p> <ul style="list-style-type: none"> Channel: 1 to 11 Security: NONE, WPA2-PERSONAL, WPA-PERSONAL, WPA2-ENTERPRISE (only for Station mode) RSSI: It is the Received signal strength indication. The range will be in db. Network configuration: IP Address, Subnet mask, Gateway address, DNS1 address, DNS2 address RX count: Packets received by WLAN TX count: Packets transferred by WLAN

Alternate Command

AT+WSTATUS

This alternate command is used to retrieve information about the current wireless status.

Synchronous Response

Table 68, page 108 describes the synchronous responses and remarks for the alternate Status command.

Table 68 Alternate Status Synchronous Responses

Responses	Remarks
MODE:<mode> CHANNEL:<channel> SSID:<ssid> BSSID:<bssid> SECURITY:<security> OK	Success The adapter reports the current network configuration to the serial host: <ul style="list-style-type: none">• Mode• Channel• SSID• BSSID• Security
NOT ASSOCIATED OK	If module is not associated with an access point.

Example 1 - Not associated state

AT+WSTATUS
NOT ASSOCIATED
OK

Example 2 - Associated state

AT+WA=GainSpanDemo,,11
IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK

AT+WSTATUS
MODE:0CHANNEL:11 SSID:"GainSpanDemo"
BSSID:98:fc:11:4a:b8:56SECURITY:NONE
OK

3.10.13 Error Code

This command is used to configure the debug level so that the response of a command will include more information (error reason) in case of an error.

Command Syntax

AT+LOGLVL=<level>

Command Note

Currently the association command (AT+WA) only supports this feature.

[Table 69, page 109](#) describes the Error Code parameters.

Table 69 Error Code Parameters

Parameter	Optional/Mandatory	Value	Description
level	Mandatory	0 (Default)	No error code or warning message along with the command response.
		1	Error code or warning message along with the command response.
		2	Error code or warning message along with the command response and buffer content which contains alternate names (domain names) provided in the incoming server certificate.

Synchronous Response

[Table 70, page 109](#) describes the synchronous responses and remarks for the Error Code command.

Table 70 Error Code Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure

3.10.14 Get RSSI

This command is used to output the current RSSI value (in dBm).

Command Syntax

AT+WRSSI=?

Synchronous Response

Table 71, page 110 describes the synchronous responses and remarks for the Get RSSI command.

Table 71 Get RSSI Synchronous Responses

Responses	Remarks
RSSI	
OK	Success

Example

AT+WRSSI=?

-33

OK

3.10.15 Set Transmit Rate

This command is used to set the transmit rate.



NOTE: This command is used for testing and debug purposes only. It is not fully functional and it is not tested for higher rates.

Command Syntax

AT+WRATE=value<Transmit rate of data frame>[,<Transmit rate of management frame>,<Transmit rate of control frame>]

Command Note

If you want to set the transmission rate to 11Mbps, then you will need to give the value as 22.

Example

AT+WRATE=22

Parameter Description

Table 72, page 111 describes the Set Transmit Rate parameters.

Table 72 Set Transmit Rate Parameters

Parameter	Optional/Mandatory	Value	Corresponding Transmission Rate	Description
Transmit rate of data frame	Mandatory	2	1 MBPS	This parameter specifies the transmission rate for data frames. If only this parameter is provided in the command, then the same value is copied for the remaining parameters Transmit rate of management frame and Transmit rate of control frame .
		4	2 MBPS	
		11	5.5 MBPS	
		13	6.5 MBPS	
		12	6 MBPS	
		18	9 MBPS	
		22	11 MBPS	
		24	12 MBPS	
		36	18 MBPS	
		39	19.5 MBPS	
		48	24 MBPS	
		52	26 MBPS	
		72	36 MBPS	
		78	39 MBPS	
		96	48 MBPS	
		104	52 MBPS	
		108	54 MBPS	
		117	58.5 MBPS	
		130	65 MBPS	
Transmit rate of management frame	Optional	Refer to the values and corresponding transmission rates in Transmit rate of data frame .		This parameter specifies the transmission rate for management frames.
Transmit rate of control frame	Optional			This parameter specifies the transmission rate for control frames.

Synchronous Response

Table 73, page 112 describes the synchronous responses and remarks for the Set Transmit Rate command.

Table 73 Set Transmit Rate Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid (if value is other than above specified value)

Example

```
AT+WRATE=2
OK
```

3.10.16 Get Transmit Rate

This command is used to obtain the current transmit rate (in ASCII format) of the data frame.



NOTE: This command is used for testing and debug purposes only. It is not fully functional and it is not tested for higher rates.

Command Syntax

```
AT+WRATE=?
```

Synchronous Response

Table 74, page 112 describes the synchronous responses and remarks for the Get Transmit Rate command.

Table 74 Get Transmit Rate Synchronous Responses

Responses	Remarks
WRATE OK	Success
WRATE 0	Module will return one of the values listed in Table 72, page 111.

Example

```
AT+WRATE=?
0
OK
```

3.10.17 Set Retry Count

This command is used to set the current retry count set to the supplied value.

Command Syntax

AT+WRETRY=<n>

Parameter Description

Table 75, page 113 describes the Set Retry Count parameters.

Table 75 Set Retry Count Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	1 to 255 Default value - 8	The current wireless retry count is set to the supplied value. The transmission retry count determines the maximum number of times a data packet is retransmitted, if an 802.11 ACK is not received.

Note: The count includes the initial transmission attempt.

Synchronous Response

Table 76, page 113 describes the synchronous responses and remarks for the Set Retry Count command.

Table 76 Set Retry Count Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid (If value is more than 1 to 255)

Example

```
AT+WRETRY=5
OK
```

3.10.18 Get Client Information

This command is used to get information about the clients associated to the module when it acts as a limited AP.

Command Syntax

AT+APCLIENTINFO=?

Synchronous Response

Table 77, page 114 describes the synchronous responses and remarks for the Get Clients Information command.

Table 77 Get Clients Information Synchronous Responses

Responses	Remarks
No. Of Stations Connected=<NoOfClients> No MacAddr IP <no> <MAC addrs> OK	Success Limited AP mode: MAC address and the IP of each of the client associated to the Limited AP. The IP address will be the one assigned to the client using DHCP.
No.Of Stations Connected=0 OK	No clients are connected.
ERROR:INVALID INPUT	If mode is not set (AT+WM) before issuing this command.

Example 1

```
AT+APCLIENTINFO=?  
No.OfStationsConnected=1
```

No	MacAddr	IP
1	60:67:20:3f:10:30	192.168.44.12
OK		

Example 2 - Client assigned with the IP statically

```
AT+APCLIENTINFO=?  
No.OfStationsConnected=1  
NO      MacAddr          IP  
1       60:67:20:3f:10:e0  *****  
OK
```



NOTE: In case the GS node has not issued the IP to the client, (client did not request for IP/client assigned with the IP statically), “****” is displayed.

3.11 WiFi Security Configuration

3.11.1 Authentication Mode

This command is used to configure the authentication mode.

Command Syntax AT+WAUTH=n

Parameter Description

Table 78, page 115 describes the WiFi Security Configuration Authentication Mode parameters.

Table 78 WiFi Security Configuration Authentication Mode

Parameter	Optional/Mandatory	Value	Mode	Description
n	Mandatory	0 (default)	None	This authentication mode command is specific to WEP encryption. If WPA/WPA2 operation is employed, the authentication mode may be left at the default value “None.”
		1	WEP Open	
		2	WEP Shared	

Synchronous Response

Table 79, page 115 describes the synchronous responses and remarks for the WiFi Security Configuration Authentication Mode command.

Table 79 WiFi Security Configuration Authentication Mode Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid. (n value is other than 0, 1, and 2)

Example

AT+WAUTH=0

OK

3.11.2 Security Configuration

This command is used to configure the GS node with different security configuration.

Command Syntax

AT+WSEC=n

Parameter Description

Table 80, page 116 describes the Security Configuration parameters.

Table 80 Security Configuration Parameters

Parameter	Optional/Mandatory	Value	Mode	Description
n	Mandatory	0 (default)	Auto security (All)	The S2W adapter supports either one of the Values. This strict security compliance is not applicable for WPS feature.
		1	Open security	
		2	WEP security	
		4	WPA-PSK security	
		8	WPA2-PSK security	
		16	WPA Enterprise	
		32	WPA2 Enterprise	
		64	WPA2-AES+TKIP security	

Synchronous Response

Table 81, page 116 describes the synchronous responses and remarks for the Security Configuration command.

Table 81 Security Configuration Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid. (n value is other than above mentioned value)

Example - GS node is configured with WEP shared security

AT+WAUTH=2

OK

AT+WSEC=2

OK

AT+WWEP1=0987654321

OK

AT+WA=GainSpanDemo,,11

IP SubNet Gateway

192.168.1.99:255.255.255.0:192.168.1.1

OK

3.11.3 WEP Keys

This command is used to configure WEP security. Upon receiving a valid command, the relevant WEP key is set to the value provided.

Command Syntax

AT+WWEPn=<key>

Parameter Description

Table 82, page 117 describes the WEP Keys parameters.

Table 82 WEP Keys Parameters

Parameter	Optional/Mandatory	Value	Description
n, key	Mandatory	N/A	<p><i>n</i> is the key index, between 1 and 4, and keys are either 10 or 26 hexadecimal digits corresponding to a 40-bit or 104-bit key.</p> <p>Last issued key will be the active key used for encryption and decryption.</p>

Synchronous Response

Table 83, page 117 describes the synchronous responses and remarks for the WEP Keys command.

Table 83 WEP Keys Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid. (<i>n</i> value is other than 1,2,3, and 4 or key is invalid)

Example - WEP shared

AT+WAUTH=2
OK

AT+WSEC=2
OK

AT+WWEP1=1122334455
OK

AT+WA=GainSpanDemo,,11
IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK

3.11.4 WEP Key Type Configuration

This command is used to enable or disable the WEP key value entered.

Command Syntax

AT+WWEPCONF=<enable/disable (1/0)>

Parameter Description

Table 84, page 118 describes the WEP Key Type Configuration parameters.

Table 84 WEP Key Type Configuration Parameters

Parameter	Optional/Mandatory	Value	Description
enable	Mandatory	1	This is ASCII mode, the WEP key entered via the AT+WWEPn=<key> command should be characters whose ASCII value is getting stored.
disable	Mandatory	0 (default)	The default value is disabled so that WEP key command accepts only HEX values.

3.11.5 WPA-PSK and WPA2-PSK Passphrase

This command is used to set the WPA-PSK and WPA2-PSK passphrase. Upon receiving the command, the PSK passphrase is reset to the value provided.



NOTE: It is recommended to use AT+WPAPSK command instead of the following command. See 3.11.6 WPA-PSK and WPA2-PSK Key Calculation, page 120.

Command Syntax

AT+WWPA=<passphrase>

Parameter Description

Table 85, page 118 describes the WPA-PSK and WPA2-PSK Passphrase parameters.

Table 85 WPA-PSK and WPA2-PSK Passphrase Parameters

Parameter	Optional/Mandatory	Value	Description
passphrase	Mandatory	8-63	The passphrase is a string containing between 8 and 63 ASCII characters, used as a seed to create the WPA <i>pre-shared</i> key (PSK). If the comma (,) is a part of the passphrase, the passphrase parameter is to be framed in double quotation marks ("phassphrase"). See 2.6.3 SSID and Passphrase, page 51 for details.

Synchronous Response

Table 86, page 119 describes the synchronous responses and remarks for the WPA-PSK and WPA2-PSK Passphrase command.

Table 86 WPA-PSK and WPA2-PSK Phassphrase Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Invalid passphrase

Example

AT+WWPA=test12345

OK

AT+WA=GainSpanDemo,,11

IP SubNet Gateway

192.168.1.99:255.255.255.0:192.168.1.1

OK

3.11.6 WPA-PSK and WPA2-PSK Key Calculation

This command is used to compute and store the value of the WPA/WPA2 PSK, derived from the SSID and Passphrase values. Computation of the PSK from the passphrase is complex and consumes substantial amounts of time and energy. To avoid recalculating this quantity every time the adapter associates, the adapter provides the capability to compute the PSK once and store the resulting value. The key value is stored in the SRAM copy of the current profile; the profile needs to be saved in flash memory for this value to persist during a transition to Standby.

Command Syntax

AT+WPAPSK=<SSID>,<passphrase>

Parameter Description

Table 87, page 120 describes the WPA-PSK and WPA2-PSK Key Calculation parameters.

Table 87 WPA-PSK and WPA2-PSK Key Calculation Parameters

Parameter	Optional/Mandatory	Value	Description
SSID	Mandatory	1-32	The SSID is a string of between 1 and 32 ASCII characters. See 2.6.3 SSID and Passphrase, page 51 .
PASSPHRASE	Mandatory	8-63	The passphrase is a string containing between 8 and 63 ASCII characters used as a seed to create the WPA <i>pre-shared key</i> (PSK). See 2.6.3 SSID and Passphrase, page 51 .

Synchronous Response

Table 88, page 120 describes the synchronous responses and remarks for the WPA-PSK and WPA2-PSK Calculation command.

Table 88 WPA-PSK and WPA2-PSK Calculation Synchronous Responses

Responses	Remarks
Computing PSK from SSID and Passphrase	Success The GS node immediately responds with this message along with standard OK response (0 in non-verbose). The current profile parameters PSK Valid, PSK-SSID, and WPA Passphrase are updated and can be queried with AT&V (see 3.9.5 Output Current Configuration, page 91). The next time the adapter associates to the given SSID, the PSK value is used without being recalculated.
OK	After the PSK has been computed, the command AT&W (to save the relevant profile) and AT&Y (to ensure that the profile containing the new PSK is the default profile) should be issued. The PSK will then be available when the adapter awakens from Standby mode. See 3.9.3 Selection of Default Profile, page 89 for profile management.
ERROR:INVALID INPUT	If parameters are not valid.

Example

```

AT+WPAPSK=GainSpanDemo,test12345
Computing PSK from SSID and PassPhrase...
OK

AT+WA=GainSpanDemo,,11
IP           SubNet           Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK

AT&W0
OK
AT+PSSTBY=1000

Out of StandBy-Timer

AT+WA=GainSpanDemo,,11
IP           SubNet           Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK

```

3.11.7 WPA-PSK and WPA2-PSK Key

This command is used to configure the WPA/WPA2 PSK key directly. This command directly sets the pre-shared key as provided. The argument is a 32-byte key, formatted as an ASCII hexadecimal number; any other length or format is considered invalid.

Command Syntax

AT+WPSK=<PSK>

Parameter Description

Table 89, page 121 describes the WPA-PSK and WPA2-PSK Key parameters.

Table 89 WPA-PSK and WPA2-PSK Key Parameters

Parameter	Optional/Mandatory	Value	Description
PSK	Mandatory	32 byte key	PSK is a 32 byte key, formatted as an ASCII hexadecimal number, and other length or format is considered invalid.

Synchronous Response

Table 90, page 122 describes the synchronous responses and remarks for the WPA-PSK and WPA2-PSK Key command.

Table 90 WPA-PSK and WPA2-PSK Key Synchronous Responses

Responses	Remarks
OK	Success After the PSK has been entered, the commands AT&W (to save the relevant profile) and AT&Y (to ensure that the profile containing the new PSK is the default profile) should be issued. The PSK will then be available when the adapter awakens from Standby. See 3.9.3 Selection of Default Profile, page 89 for more information on profile management.
ERROR:INVALID INPUT	Invalid PSK (if PSK is not 32 bytes)

Example

AT+WPSK=0001020304050607080900010203040506070809000102030405060708090001

OK

AT&W0

OK

AT+WA=GainSpanDemo,,11

IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1

OK

AT+PSSTBY=1000

Out of StandBy-Timer

AT+WA=GainSpanDemo,,11

IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1

OK

3.11.8 EAP-Configuration

This command is used to set the GS node to the Outer authentication, Inner authentication, user name and password for EAP security.

Command Syntax

```
AT+WEAPCONF=<Outer Authentication>,<Inner  
Authentication>,<user name>,<password>[,<PEAP with  
certificate>]
```

Parameter Description

Table 91, page 123 describes the EAP Configuration parameters.

Table 91 EAP Configuration Parameters

Parameter	Optional/Mandatory	Value	Description	
Outer Authentication		The valid outer authentication values are:		
Outer Authentication	Mandatory	43	EAP-FAST	
		13	EAP-TLS	
		21	EAP-TTLS	
		25	EAP-PEAP	
user name	Mandatory Note: This parameter is not applicable for EAP-TLS.	N/A	The user name is an ASCII string with a maximum length of 32 ASCII characters.	
password	Mandatory Note: This parameter is not applicable for EAP-TLS.	N/A	The password is an ASCII string with a maximum length of 32 ASCII characters.	
PEAP with certificate	Optional	1	PEAP with certificate is an optional parameter which will be set to 1 to add PEAP certificates.	

Synchronous Response

Table 92, page 124 describes the synchronous responses and remarks for the EAP-Configuration command.

Table 92 EAP-Configuration Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Invalid parameters

Example 1- PEAP without certificates

AT+WEAPCONF = 25,26,gsn,GainSpanDemo123

OK

AT+SETTIME=15/10/2013,17:31:00

OK

AT+WA=GainSpanDemo,,11

IP SubNet Gateway

192.168.1.99:255.255.255.0:192.168.1.1

OK

AT+NDHCP=1

IP SubNet Gateway

192.168.23.103:255.255.255.0:192.168.23.1

OK

Example 2 - PEAP with certificates set to the optional parameter 1

AT+WEAPCONF=25,26,gsn,GSDemo123,1" (PEAPv0 with Certificate)

AT+WEAPCONF=25,6,gsn,GSDemo123,1" (PEAPv1 with Certificate)

3.11.9 EAP

This command is used to enable the GS node to receive the EAP-TLS certificates.

Command Syntax

AT+WEAP=<Type>,<Format>,<Size>,<Location><CR><ESC>W <data of size above>

Parameter Description

Table 93, page 125 describes the EAP parameters.

Table 93 EAP Parameters

Parameter	Optional/Mandatory	Value	Description
Type	Mandatory	Type of the certificate	
		0	CA certification
		1	Client certification
		2	Private key
Format	Mandatory	Format of the certificate	
		0	Binary
		1	Hex
Size	Mandatory	Size of the certificate to be transferred	
Location	Mandatory	Location to store the certificates	
		0	Flash
		1	RAM

Note: There is a carriage return after <location>.

Synchronous Response

Table 94, page 125 describes the synchronous responses and remarks for the EAP command.

Table 94 EAP Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Invalid parameters

Example - Configuring to receive Client CA

Type:0 (Client CA)
Format:0 (Binary)
NumberofBytes:3026

AT+WEAP=0,0,3026,0
OK
<ESC>W

From the Tera Term VT, perform the following:

1. Select File > Send file
2. Select the check box Binary under Option
3. Open the folder which contains the ClientCA certificate
4. Select ClientCA (this has 3026 bytes of data)

3.11.10 EAP Time Validation

This command is used to enable or disable time validation for EAP certificates.

NOTE: To disable CA validation, do not load CA cert.

Command Syntax

AT+WEAPTIMECHK=n

Parameter Description

Table 93, page 125 describes the EAP time validation parameters.

Table 95 EAP Time Validation Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0	Disable
		1	Enable (Default)

Synchronous Response

Table 94, page 125 describes the synchronous responses and remarks for the EAP time validation command.

Table 96 EAP Time Validation Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Invalid parameters

3.11.11 Certificate Addition

This command is used to add the certificate for SSL/HTTPS and EAP connections.

Command Syntax

AT+TCERTADD=<Name>,<Format>,<Size>,<Location>

After receiving OK, execute the following Escape sequence and perform the remaining steps in Tera Term as mentioned below:

<ESC>W

From the Tera Term VT, perform the following:

1. Select File > Send file
2. Select the check box Binary under Option
3. Open the folder which contains the certificates

Parameter Description

Table 97, page 128 describes the Certificate Addition parameters.

Table 97 Certificate Addition Parameters

Parameter	Optional/Mandatory	Value	Description
Name	Mandatory	Name of a certificate should be prefixed with SSL_ or ssl_ . Example: abc.der should be renamed to ssl_abc.der . Note: Certificates are also uploaded or deleted over the air through the interface provided in <code>sslcert.html</code> . The naming convention mentioned above shall apply there as well.	This parameter specifies the name of the certificate to be added. Note: ‘SSL_CA’, ‘SSL_SERVER’ and ‘SSL_KEY’ should not be used as names as they are reserved for HTTPS server certificates (root certificate is used to validate the clients, server certificate and server key respectively).
Format	Mandatory	0,1 0: Binary (der format) 1: Hexadecimal (pem format)	Format of the certificate to be added.
Size	Mandatory	N/A	Size of the certificate to be added.
Location	Mandatory	Location to store the certificates 0 1	Flash RAM

Note: There is a carriage return after the <Location> parameter.

Synchronous Response

Table 98, page 129 describes the synchronous responses and remarks for the Certificate Addition command.

Table 98 Certificate Addition Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Invalid parameters

Example

```
Name:CA
Format:0 (Binary)
Size:868 bytes
Location:0 (Flash)
```

```
AT+NDHCP=1
```

```
OK
```

```
AT+WA=GainSpanDemo
IP           SubNet          Gateway
192.168.44.148:255.255.255.0:192.168.44.1
OK
AT+TCERTADD=ca,0,868,0
OK
```

```
<ESC>W
```

From the Tera Term VT, perform the following:

1. Select File > Send file
2. Select the check box Binary under Option
3. Open the folder which contains the certificate ca which is of 868 bytes.

3.11.12 Certificate Deletion

This command is used to delete the SSL/HTTPS/EAP-TLS certificate that is stored in Flash/RAM by name.

Command Syntax AT+TCERTDEL=<certificate name>

Parameter Description

Table 99, page 130 describes the Certificate Deletion parameters.

Table 99 Certificate Deletion Parameters

Parameter	Optional/Mandatory	Value	Description
certificate name	Mandatory	N/A	Name of the certificate to delete from Flash/RAM. In case of EAP-TLS certificate names are: <ul style="list-style-type: none">• TLS-CA• TLS-CLIENT• TLS-KEY

Synchronous Response

Table 100, page 130 describes the synchronous responses and remarks for the Certificate Deletion command.

Table 100 Certificate Deletion Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Invalid parameter

Example

AT+TCERTDEL=TLS+CA

OK

3.11.13 Certificate Validation

This command is used to enable or disable Server's certificate validation on DUT.



NOTE: This command is used for SSL only. The command configuration is not retained across standby.

Command Syntax AT+SRVVALIDATIONEN=n

Parameter Description

Table 93, page 125 describes the certificate validation parameters.

Table 101 Certificate Validation Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0 - Disable	It disables Server's certificate validation on DUT.
		1 - Enable (Default)	It enables Server's certificate validation on DUT.

Synchronous Response

Table 94, page 125 describes the synchronous responses and remarks for the certificate validation command.

Table 102 Certificate Validation Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Invalid parameters

3.11.14 Radio Receiver in Active Mode

This command is used to enable/disable the 802.11 radio receiver. This minimizes latency and ensures that packets are received at the cost of increased power consumption. The GainSpan SoC cannot enter Deep Sleep (see [3.20.1 Enable Deep Sleep, page 246](#)) even if it is enabled (AT+PDPSLEEP). The Power Save mode (see [3.11.15 Radio Receiver in Power Save Mode, page 133](#)) can be enabled but will not save power, since the receiver is left on.

Command Syntax AT+WRXACTIVE=n

Parameter Description

[Table 103, page 132](#) describes the Enable/Disable 802.11 Radio parameters.

Table 103 Enable/Disable 802.11 Radio Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0 (default)	802.11 radio receiver is off
		1	802.11 radio receiver is always on

Synchronous Response

[Table 104, page 132](#) describes the synchronous responses and remarks for the Enable/Disable 802.11 Radio command.

Table 104 Enable/Disable 802.11 Radio Synchronous Responses

Responses	Remarks
OK	Success
ERROR: INVALID INPUT	Invalid parameter (If n value is other than 0 or 1)



NOTE: The number of times radio is enabled using AT+WRXACTIVE, that many times has to be disabled.

Example AT+WRXACTIVE=1

OK

AT+WRXACTIVE=1

OK

AT+WRXACTIVE=0

OK

AT+WRXACTIVE=1

OK

Example Use Case 1 Radio receiver is always on, Power Save mode is enabled but will not save power since the receiver is left on.

```
AT+WRXACTIVE=1
OK
```

```
AT+WRXPS=1
OK
```

Example Use Case 2 The receiver is switched off. The node will not receive any packets at this time.

```
AT+WRXACTIVE=0
OK
```

```
AT+WRXPS=0
OK
```

3.11.15 Radio Receiver in Power Save Mode

This command is used to enter Power Save Mode. Once enabled, radio will be switched off (after informing AP) when ever possible (e.g., in between beacons intervals, when there is no data transmission). Since module inform up about its inactivity, AP shall buffer all the incoming unicast traffic during this time.



NOTE: Refer to the AT+WIEEEPSPOLL command for 802.11 power save mode.

Command Syntax

AT+WRXPS=n

Parameter Description

Table 105, page 133 describes the Enable/Disable 802.11 Power Save Mode parameters.

Table 105 Enable/Disable 802.11 Power Save Mode Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0	Power Save mode is disabled
		1 (default)	Power Save mode is enabled

Synchronous Response

Table 106, page 133 describes the synchronous responses and remarks for the Enable/Disable 802.11 Power Save Mode command.

Table 106 Enable/Disable 802.11 Power Save Mode Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid (If n value is other than 0 or 1)

Example

```
AT+WRXACTIVE=0
```

```
OK
```

```
AT+WRXPS=1
```

```
OK
```

Prior to issuing this command the radio should be of (AT+WRXACTIVE=0), otherwise there is no effect of power save, if radio receiver is on.

In this case the node will inform the Access Point that it will go to sleep, and the Access Point will buffer any packets addresses to that node. The node will awaken to listen to periodic beacons from the Access Point that contains a Traffic Indication Map (TIM) that will inform the Station if packets are waiting for it. Buffered packets can be retrieved at that time, using ***PSPoll*** commands sent by the node. In this fashion, power consumed by the radio is reduced (although the benefit obtained depends on traffic load and beacon timing), at the cost of some latency. The latency encountered depends in part on the timing of beacons, set by the Access Point configuration. Many Access Points default to 100msec between beacons; in most cases this parameter can be adjusted.

3.11.16 Enable/Disable Multicast Reception

This command is used to enable or disable Multicast and Broadcast reception. Multicast and Broadcast are tied together.

Command Syntax

AT+MCSTSET=n

Parameter Description

Table 107, page 135 describes the Enable/Disable Multicast Reception parameters.

Table 107 Enable/Disable Multicast Reception Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0	<p>Disable 802.11 MAC layer multicast + broadcast reception is disabled.</p> <p>Reception of all higher layer (IP and above) multicast and broadcast packets are disabled by AT+MCSTSET=0 option. When disabled, the ability for the node to receive higher layer broadcast traffic such as ARP responses that are needed to establish IP layer communication is also disabled.</p>
		1 (default)	<p>Enable 802.11 MAC layer multicast + broadcast reception is enabled.</p> <p>Reception of all higher layer (IP and above) multicast and broadcast packets is enabled by “AT+MCSTSET=1” option. The MCU will receive/transmit the multicast and broadcast packets by opening the UDP sockets using the command “AT+NCUDP” (see 3.13.4 UDP Clients for IPv4, page 183).</p>

Synchronous Response

Table 108, page 135 describes the synchronous responses and remarks for the Enable/Disable Multicast Reception command.

Table 108 Enable/Disable Multicast Reception Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid (If n value is other than 0 or 1)

Example Use Case

Table 109, page 136 lists the use cases for the Enable/Disable Multicast Reception.

Table 109 Enable/Disable Multicast Reception

No.	Power Save Parameter	Listen Beacon Parameter	Listen Multicast Parameter	Radio State
1	AT+WRXACTIVE=1	Don't Care	Don't Care	Radio is always ON.
2	AT+WRXACTIVE=1	AT+WRXPS=0	Don't Care	Setting Not Valid - Radio will be always ON.
3	AT+WRXACTIVE=0	AT+WRXPS=0	Don't Care	Setting Not Valid - Radio will be in PS mode turning ON and OFF every listen interval or DTIM depending on "listen multicast" setting.
4	AT+WRXACTIVE=0	AT+WRXPS=1	Disable	Radio is turned ON based on listen interval. See below for listen interval setting.
5	AT+WRXACTIVE=0	AT+WRXPS=1	Enable	Radio is turned ON based on DTIM interval and listen interval setting.

Example Use Case 1 - Where - Destination address (Multicast): 224.0.0.0**Configuring**

**GainSpan node as a UDP Client and Transmitting/
Receiving Multicast Packets**

Destination port: 3610

AT+WA=GainSpanDemo,,11

IP SubNet Gateway

192.168.1.99:255.255.255.0:192.168.1.1

OK

AT+NDHCP=1

IP SubNet Gateway

192.168.23.101:255.255.255.0:192.168.23.1

OK

AT+MCSTSET=1

OK

AT+NCUDP=224.0.0.0,3610

CONNECT 0

OK

Example Use Case 2 - Where - Destination address: 192.168.23.100 (Unicast)**Configuring**

**GainSpan node as a UDP Client and Transmitting/
Receiving Unicast Packets**

Destination port: 9000

AT+WA=GainSpanDemo,,11

IP SubNet Gateway

102.168.23.101:255.255.255.0:192.168.23.1

OK

AT+MCSTSET=1

OK

AT+NCUDP=192.168.23.100,9000

CONNECT 0

OK

3.11.17 Sync Loss Interval

This command is used to set the adapter for sync loss interval for n times the beacon interval so that if the GainSpan node does not receive the beacon for this time, it informs the user this event is “Disassociation event.”

Command Syntax

AT+WSYNCINTRL=<n>

Parameter Description

Table 110, page 138 describes the Sync Loss Interval parameters.

Table 110 Sync Loss Interval Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	1-63325	<i>n</i> is the number of beacon intervals.
		100 (default)	The module accepts the values of range 1-65535 Width default value 100 beacons

Synchronous Response

Table 111, page 138 describes the synchronous responses and remarks for the Sync Loss Interval command.

Table 111 Sync Loss Interval Asynchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Invalid parameter (out of range)

Asynchronous Response

Table 112, page 138 describes the asynchronous responses and remarks for the Sync Loss Interval command.

Table 112 Sync Loss Interval Asynchronous Responses

Responses	Remarks
314Disassociation Event Whee: Subtype - 3 Length - 14 (ASCII equivalent decimal is 20 characters, i.e., length of the actual message) Actual message - Disassociation Event The type of message. Length is 1 byte. for asynchronous message, it is 0x41 (ASCII value A). Note: <ESC> and Type is not displayed because its Tera Term issue.	GainSpan node does not receive beacons for this time informs the user with this message.

Example

AT+WSYNCINTRL=500

3.11.18 Association Keep Alive Timer

This command is used to keep-alive the timing intervals associated with the adapter. This keep-alive timer will fire for every n seconds once the adapter is associated. This timer will keep the adapter in associated state even when there is no activity between AP and adapter.

Command Syntax

AT+PSPOLLINTRL=<n>

Parameter Description

Table 113, page 139 describes the Association Keep Alive Timer parameters.

Table 113 Association Keep Alive Timer Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0 to 255 seconds 0 (default)	When set to 0, the Keep alive timer is disabled. If disabled, then the keep alive timer will fire for every 45 seconds.

Synchronous Response

Table 114, page 139 describes the synchronous responses and remarks for the Association Keep Alive Timer command.

Table 114 Association Keep Alive Timer Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid

Example Use Case

AT+WA=GainSpanDemo

```
IP           SubNet           Gateway
192.168.17.14:255.255.255.0:192.168.17.1
OK
```

```
AT+NDHCP=1
IP           SubNet           Gateway
192.168.17.14:255.255.255.0:192.168.17.1
OK
```

```
AT+PSPOLLINTRL=60
OK
```

3.11.19 IEEE PS Poll Listen Interval

This command is issued once to configure the mode (DTIM based wakeup, Listen interval based wake up or Custom wake up) and then to enable the configuration (in commands issued when configured for listen interval based wakeup). Configuration is to be issued only once and then enable/disable can be done at run time to control radio.

Command Syntax

```
AT+WIEEEPSPOLL=<enable>[,listenInterval][,wakeupType]  
[,wakeupInterval][,BeaconWaitTimeout][,DataRxType][,Activ  
eToOffTimeout][,SwitchToActivePeriod]
```

Parameter Description

Table 115, page 140 describes the IEEE PS Poll Listen Interval parameters.

Table 115 IEEE PS Poll Listen Interval Parameters

Parameter	Optional/Mandatory	Value	Description
enable	Mandatory	0	Disable IEEE PS
		1	Enable IEEE PS (wakeupType tells whether DTIM or Listen interval)
		2	Configure IEEE PS
Note: enable/disable is used run-time to control radio while remaining parameters will be used only for configuration when required. If configuration is not specified, last configuration will be used.			
listenInterval	Optional (if n is enabled then this parameter is valid)	1-65535	The GS node will set the listen interval for n beacons. Although this is a 16-bit value, the maximum recommended is 10-bit.
WakeupType	Optional (valid if wakeup type is listen interval and custom)	0	DTIM based wakeup
		1	Listen Interval based wakeup
		2	Custom wakeup
wakeupInterval	Optional	10ms (default)	Wakeup Interval to be used for listening to beacons if it is custom wakeup.
BeaconWaitTimeout	Optional	beacon interval	Maximum time allowed to wait for beacon reception after wakeup.
DataRxType	Optional	0	Receive buffered data using Legacy PS-POLL or WMM UAPSD, whatever AP supports.
		1	Switch to active mode to receive buffered data.

Table 115 IEEE PS Poll Listen Interval Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
ActiveToOffTimeout	Optional	N/A	Time to be in active radio state if DataRxType is switched to active mode. Time is extended whenever a frame is received and radio state is turned off after timeout. A null frame is sent to AP to indicate transition to doze state.
SwitchToActivePeriod	Optional	N/A	Time in milliseconds after which DUT switches to Active state even though TIM bit is not set in AP.

Note: All the *Optional* parameters need to be configured with their default values.

Command Note	The radio of the STA can be controlled only with 3 AT commands for GS2000 based modules. They are AT+WRXACTIVE, AT+WRXPS, and AT+WIEEEPSPOLL.
Example - AT+WRXACTIVE	If AT+WRXACTIVE = 1, then the radio is always ON. No power save is done in this case. Regardless of what the parameters for the other two commands are, the radio will receive all the packets. Rest of the commands are “Don’t Care.”
Example - AT+WRXPS	If AT+WRXPS = 1, Regardless of what the parameters for AT+WIEEEPSPOLL are, the STA will wake up for every beacon. AT+WIEEEPSPOLL is a “Don’t Care” in this case. If AT+WRXPS = 0, the STA will not wake up for every beacon. Based on the AT+WIEEEPSPOLL, the wake will be decided as explained further.
Example - AT+WIEEEPSPOLL	This command can be used for three purposes: <ul style="list-style-type: none"> – To configure the Power Save behavior – To Enable the Power Save – To Disable the Power Save
Usage - Configuration of Power Save	To configure the Power Save behavior on the STA, the first parameter of the command should be 2. The STA can be configured in 3 ways: <ul style="list-style-type: none"> – Wake up for Listen Interval – Wake up for DTIM – Wake up for a custom number of beacons
Wake up for Listen Interval	To configure the STA to wake up for the listen interval, the command is AT+WIEEEPSPOLL=2,10,1. This means that the STA will advertise in the Association Request that the listen interval will be for every 10 beacons. Once associated, the STA will wake up for every 10 beacons.
Wake up for DTIM	To configure the STA to wake up for every DTIM interval, the command is AT+WIEEEPSPOLL=2,,0. Here we did not specify the listen interval as that will be the default. In this case, the STA will advertise the default Listen Interval in the Association

Request. Once associated, the STA will wake up for every DTIM interval that has been configured on the AP.

Custom Wake up

To configure the STA to wake up at a custom interval, the command is AT+WIEEEPSPOLL=2,,2,5. Here also, we did not specify the listen interval, that will be the default. The STA will advertise the default Listen Interval in the Association Request. Once associated, the STA will wake up for every 5 beacons.

Difference between Listen Interval based Wake up Versus Custom Wake up

At the outset, both of these options do the same thing - to wake the STA based on the number of beacons given.

Either of these options can be used to wake the STA. However, the use case is as follows:

Example Use Case

Whenever the STA is needed to wake up at some configured interval, the Custom Wake up option should be used. While configuring the custom wake up parameters, the listen interval should not be entered; the default listen interval will be used in the association request. Usually, in the association request, the STA will advertise the listen interval as a large value (e.g., 10 beacons). The configuration of the custom wake up interval will be less than the listen interval (e.g., 5 beacons). In this case, the STA bluffs to the AP while associating telling that it will wake up for every 10 beacons. But, in reality, it will wake up for every 5 beacons. This is just to ensure that the AP shouldn't drop the buffered frames in case the PS Poll request from the STA does not reach the AP.

Enable Power Save

To enable the power save on the STA, the command is AT+WIEEEPSPOLL=1. Whenever AT+WIEEEPSPOLL is given as 1, the STA will take the last power save configuration into effect. So, the user should first configure the behavior and then enable the power save.

Disable Power Save

To disable the power save on the STA, the command is AT+WIEEEPSPOLL=0. When this command is executed, the radio is fully off. Order of Precedence between commands - WRXACTIVE > WRXPS > WIEEEPSPOLL.

Command Note

If the power save behavior is changed after the association is done, the new changes will take into effect only for the next association.

3.11.20 WLAN Keep Alive Interval

This command is used to set the keep-alive interval for *n* seconds. This keep-alive timer will fire for every *n* seconds once the node is associated. This timer will keep the node in associated state even if there is no activity between AP and GainSpan node.

Command Syntax

AT+WKEEPALIVE=<n>

Parameter Description

[Table 116, page 143](#) describes the WLAN Keep Alive Interval parameters.

Table 116 WLAN Keep Alive Interval Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0 to 255 seconds	The module accepts the values of range 0 to 255 (units are in seconds).
		45 seconds (default)	The default keep alive timer value is 45 seconds. The value 0 disables this feature.

Synchronous Response

[Table 117, page 143](#) describes the synchronous responses and remarks for the WLAN Keep Alive Interval command.

Table 117 WLAN Keep Alive Interval Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid

3.12 Network Interface

3.12.1 DHCP Client Support for IPv4

This command is used to enable or disable DHCP client support for IPv4 network.

Command Syntax AT+NDHCP=n [,<hostname>,<radio mode>,<lease period>,<retry interval>]

Parameter Description

Table 118, page 144 describes the DHCP Client Support for IPv4 parameters.

Table 118 DHCP Client Support for IPv4 Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0 (default)	Disable
		1	Enable
hostname	Optional	N/A	<i>hostname</i> is a string with a maximum character length of 15. This will be displayed by Access Points as the hostname in the DHCP Clients table.
radio mode	Optional	1	Active mode
		2 (default)	PS poll mode
		3	IEEE PS poll mode (It is the PS mode configured using AT+WIEEEPSPOLL command.)
lease period	Optional	4294967296 seconds - infinite seconds (default)	It specifies the lease period to be requested in DHCP discover message.
retry interval	Optional	2 seconds	It specifies the time interval between successive DHCP retries.

Synchronous Response

Table 119, page 145 describes the synchronous responses and remarks for the DHCP Client Support for IPv4 command.

Table 119 DHCP Client Support for IPv4 Synchronous Responses

Responses	Remarks
OK	Success If the Adapter is not associated when the command is received, future associations will attempt to employ DHCP.
IP SubNet Gateway <IPAddress> <SubNet address> <Gateway address>	Success If the interface is associated with a network, enabling DHCP will cause an attempt to obtain an IP address using DHCP from that network. Therefore issuing this command with n=1 will cause the Adapter to attempt to refresh an existing DHCP address.
IP CONFIG FAIL	If the DHCP renewal failed then the adapter closes all the sockets opened and sends an error message ERROR: IP CONFIG FAIL to the serial interface. The host can re-issue the network config command to redo the DHCP procedure again.

Asynchronous Response

Table 120, page 145 describes the asynchronous responses and remarks for the DHCP Client Support for IPv4 command.

Table 120 DHCP Client Support for IPv4 Asynchronous Responses

Responses	Remarks
815ERROR: IP CONFIG FAIL Where: Subtype - 8 Length - 15 (ASCII equivalent decimal is 21 characters, i.e., length of the actual message). Actual message - ERROR: IP CONFIG FAIL The type of message. Length is 1 byte. For asynchronous message, it is 0x41 (ASCII value A).	IP configuration has failed. This message comes asynchronously when there is a DHCP renew fails. For asynchronous message format.

Note: <ESC> and Type is not displayed because its Tera Term issue.

Example 1 - If the node is not associated when the command is received

AT+NDHCP=1
OK

**Example 2 - If the
node is associated
when the command
is received**

```
AT+WA=GainSpanDemo
IP           SubNet       Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK
```

```
AT+NDHCP=1
IP           SubNet       Gateway
192.168.44.145:255.255.255.0:192.168.44.1
OK
```

3.12.2 Static Configuration of Network Parameters for IPv4

This command is used to set network parameters statically. Upon deployment of this command, any previously specified network parameters are overridden, and the node is configured to use the newly specified network parameters for the current association, if associated, and for any future association. The use of DHCP is disabled if the network parameters are configured statically. The DNS address can be set using AT+DNSSET (see [3.12.15 Static Configuration of DNS \(Client\), page 167](#)).

Command Syntax AT+NSET=<Src Address>,<Net-mask>,<Gateway>

Parameter Description

[Table 121, page 147](#) describes the Static Configuration of Network Parameters for IPv4.

Table 121 Static Configuration of Network Parameters for IPv4

Parameter	Optional/Mandatory	Value	Description
Src Address	Mandatory	N/A	IP address of the source in the form xxx.xxx.xxx
Net-mask	Mandatory	N/A	Net mask is in the form of xxx.xxx.xxx
Gateway	Mandatory	N/A	Gateway of the address (node: Src Adr and Gateway should be same in the case of Limited AP or P2P mode)

Synchronous Response

[Table 122, page 147](#) describes the synchronous responses and remarks for the Static Configuration of Network Parameters for IPv4 command.

Table 122 Static Configuration of Network Parameters for IPv4 Synchronous Responses

Responses			Remarks
IP <IPaddress>	SubNet <SubNetaddress>:	Gateway <Gatewayaddress>	Success

Example Use Case 1 - If the node is not associated when the command is received

AT+NSET=192.168.44.12,255.255.255.0,192.168.44.12
OK
AT+WA=GainSpan
IP SubNet Gateway
192.168.44.12:255.255.255.0:192.168.44.12
OK

Example Use Case 2 - If the node is associated when the command is received

AT+WA=GainSpanDemo
IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK
AT+NSET=192.168.44.12,255.255.255.0,192.168.44.12
IP SubNet Gateway
192.168.44.12:255.255.255.0:192.168.44.12

3.12.3 MDNS Module Initialization for IPv4

This command is used to start the MDNS procedure of the node with IPv4 network.

Command Syntax AT+MDNSSTART

Synchronous Response

Table 123, page 148 describes the synchronous responses and remarks for the MDNS Module Initialization for IPv4 command.

Table 123 MDNS Module Initialization for IPv4 Synchronous Responses

Responses	Remarks
OK	Success Prior to issuing of this command the node should be associated to the network.
ERROR	Failure If the node is not associated before issuing this command.

Example AT+MDNSSTART
OK

Example - All MDNS Commands

```
AT+WA=GainSpanDemo,,11
IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK

AT+NDHCP-1
IP SubNet Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK

AT+WEBPROV=admin,admin
OK

AT+MDNSSTART
OK

AT+MDNSHNREG=Prov,local
OK

Registration Success! for RR:Prov
AT+MDNSSRVREG=Provisioning,,_http,_tcp,local,80,0,path=
/gsprov.html
OK
```

Registration Success!!for RR: Provisioning
AT+MDNSANNOUNCE
OK

AT+MDNSHNDREG=Prov, local
OK

AT+MDNSSRVDEREG=Provision,,_http,_tcp,local
OK

AT+MDNSSTOP
OK

3.12.4 MDNS Host Name Registration

This command is used to register or give a unique name to each of the nodes for MDNS.

Command Syntax AT+MDNSHNREG=[<Host name>],<Domain name>

Parameter Description

Table 124, page 150 describes the MDNS Host Name Registration parameters.

Table 124 MDNS Host Name Registration Parameters

Parameter	Optional/Mandatory	Value	Description
Host name	Optional	N/A	<i>Host name</i> is optional. If host name is not given, factory default name concatenated with last 3 bytes of the MAC address shall be taken. Maximum host name length supported is 32 bytes.
Domain name	Mandatory	N/A	The domain name is always “local.”

Synchronous Response

Table 125, page 150 describes the synchronous responses and remarks for the MDNS Host Name Registration command.

Table 125 MDNS Name Registration Synchronous Responses

Responses	Remarks
OK Registration Success!! for RR: <Host name>	Success Prior to issue this command, the node should be associated to the network.
ERROR	Failure If the node is not started in MDNS module, before issuing this command.

Example

```
AT+MDNSHNREG=Provisioning,local
OK
```

Example - All MDNS Commands

```
AT+WA=GainSpanDemo,,11
IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK
```

```
AT+NDHCP-1
IP SubNet Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK
```

```
AT+WEBPROV=admin,admin
OK
```

```
AT+MDNSSTART
OK
```

```
AT+MDNSHNREG=Prov,local
OK
```

```
Registration Success!for RR:Prov
AT+MDNSSRVREG=Provisioning,,_http,_tcp,local,80,0,path=
/gsprov.html
OK
```

```
Registration Success!!for RR: Provisioning
AT+MDNSANNOUCE
OK
```

```
AT+MDNSHNDEREG=Prov,local
OK
```

```
AT+MDNSSRVDEREG=Provision,,_http,_tcp,local
OK
```

```
AT+MDNSSTOP
OK
```

3.12.5 MDNS Host Name De-registration

This command is used to de-register the domain name which is registered using AT+MDNSHNREG.

Command Syntax

AT+MDNSHNDREG=<Host name>,<Domain name>

Parameter Description

Table 126, page 152 describes the MDNS Host Name De-Registration parameters.

Table 126 MDNS Host Name De-Registration Parameters

Parameter	Optional/Mandatory	Value	Description
Host name	Mandatory	N/A	<i>Host name</i> is the host name which is registered using AT+MDNSHNREG.
Domain name	Mandatory	N/A	<i>Domain name</i> is the domain name which is registered using AT+MDNSHNREG.

Synchronous Response

Table 127, page 152 describes the synchronous responses and remarks for the MDNS Host Name De-Registration command.

Table 127 MDNS Host Name De-Registration Synchronous Responses

Responses	Remarks
OK	Success Prior to issuing this command the node should be registered with the host name.
ERROR	Failure Before issuing this command, if the node is not registered with a host name.

Example

```
AT+MDNSHNDREG=Prov,local
OK
```

Example - All MDNS Commands

```
AT+WA=GainSpanDemo,,11
IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK
```

```
AT+NDHCP-1
IP SubNet Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK
```

```
AT+WEBPROV=admin,admin
OK
```

```
AT+MDNSSTART
OK
```

```
AT+MDNSHNREG=Prov,local
OK
```

```
Registration Success!for RR:Prov
AT+MDNSSRVREG=Provisioning,,_http,_tcp,local,80,0,path=
/gsprov.html
OK
```

```
Registration Success!!for RR: Provisioning
AT+MDNSANNOUCE
OK
```

```
AT+MDNSHNDREG=Prov,local
OK
```

```
AT+MDNSSRVDEREG=Provision,,_http,_tcp,local
OK
```

```
AT+MDNSSTOP
OK
```

3.12.6 MDNS Services Registration

This command is used to register the services to the MDNS.

Command Syntax

```
AT+MDNSSRVREG=<ServiceInstanceName>, [<ServiceSubType>], <ServiceType>, <Protocol>, <Domain>, <port>, <Default Key=Val>, <key 1=val 1>, <key 2=val 2>...
```

Parameter Description

Table 128, page 154 describes the MDNS Services Registration parameters.

Table 128 MDNS Services Registration Parameters

Parameter	Optional/Mandatory	Value	Description
ServiceInstanceName	Mandatory	256	<i>ServiceInstanceName</i> is the name of the service. It can take up to 256 characters.
ServiceSubType	Optional	N/A	<i>ServiceSubType</i> is the name of the service subtype if any.
ServiceType	Mandatory	N/A	<i>ServiceType</i> is the type of service, for example HTTP, FTP, etc.
Protocol	Mandatory	N/A	<i>Protocol</i> is the protocol used (TCP, UDP).
Domain	Mandatory	N/A	Name of the domain. It should be “local”
Port	Mandatory	N/A	Port is used for communication (80 for HTTP).
DefaultKey	Mandatory	0	No default key to be added.
		1	Provisioning
		2	Over The Air Firmware Upgrade

Note: *Default Key* is a number. GainSpan node support a two default key value pairs to be used with iPhone/Android applications.

Synchronous Response

Table 129, page 154 describes the synchronous responses and remarks for the MDNS Services Registration command.

Table 129 MDNS Services Registration Synchronous Responses

Responses	Remarks
OK Registration Success!! for RR:<ServiceInstanceName>	Success Prior to issuing this command, the node should be started with a MDNS module.
ERROR	Failure Command AT+MDNSSRVREG is issued. Before issuing AT+MDNSSTART (i.e, the node is not started with an MDNS module)

Example Use Case - GainSpan node is configured with mDNS module with custom key value

Where - Default key - 0 (Number 0 indicates no default key value to be added)

```
AT+MDNSSRVREG=prov,,_http,_tcp,local,80,0,  
SSID=GainSpanDemo,Channel=6  
OK
```

Example - All MDNS Commands

```
AT+WA=GainSpanDemo,,11  
IP SubNet Gateway  
192.168.1.99:255.255.255.0:192.168.1.1  
OK
```

```
AT+NDHCP-1  
IP SubNet Gateway  
192.168.23.101:255.255.255.0:192.168.23.1  
OK
```

```
AT+WEBPROV=admin,admin  
OK
```

```
AT+MDNSSTART  
OK
```

```
AT+MDNSHNREG=Prov,local  
OK
```

```
Registration Success!for RR:Prov  
AT+MDNSSRVREG=Provisioning,,_http,_tcp,local,80,0,path=  
/gsprov.html  
OK
```

```
Registration Success!!for RR: Provisioning  
AT+MDNSANNOUCE  
OK
```

```
AT+MDNSHNDEREG=Prov,local  
OK
```

```
AT+MDNSSRVDEREG=Provision,,_http,_tcp,local  
OK
```

```
AT+MDNSSTOP  
OK
```

3.12.7 MDNS Services De-Registration

This command is used to de-register the services which are registered through AT+MDNSSRVDERREG.

Command Syntax

AT+MDNSSRVDEREG=<ServiceInstanceName>, [<ServiceSubType>],
<ServiceType>, <Protocol>, <Domain>

Parameter Description

Table 130, page 156 describes the MDNS Services De-Registration parameters.

Table 130 MDNS Services De-Registration Parameters

Parameter	Optional/Mandatory	Value	Description
ServiceInstanceName	Mandatory	256	<i>ServiceInstanceName</i> is the name of the service. It can take up to 256 characters.
ServiceSubType	Optional	N/A	<i>ServiceSubType</i> is the name of the service subtype if any.
ServiceType	Mandatory	N/A	<i>ServiceType</i> is the type of service, for example HTTP, FTP, etc.
Protocol	Mandatory	N/A	<i>Protocol</i> is the protocol used (TCP, UDP).
Domain	Mandatory	N/A	Name of the domain. It should be “local”

Synchronous Response

Table 131, page 156 describes the synchronous responses and remarks for the MDNS Services De-Registration command.

Table 131 MDNS Services De-Registration Synchronous Responses

Responses	Remarks
OK	Success Prior to issuing this command, the node should be registered with the MDNS service through AT+MDNSSRVREG.
ERROR	Failure Before issuing this command, the node is not registered with MDNS module.

Example

```
AT+MDNSSRVDEREG=Prov,,,_http,_tcp,local
OK
```

Example - All MDNS Commands

```
AT+WA=GainSpanDemo,,11
IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK
```

```
AT+NDHCP-1
IP SubNet Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK
```

```
AT+WEBPROV=admin,admin
OK
```

```
AT+MDNSSTART
OK
```

```
AT+MDNSHNREG=Prov,local
OK
```

```
Registration Success!for RR:Prov
AT+MDNSSRVREG=Provisioning,,,_http,_tcp,local,80,0,path=
/gsprov.html
OK
```

```
Registration Success!!for RR: Provisioning
AT+MDNSANNOUCE
OK
```

```
AT+MDNSHNDEREG=Prov,local
OK
```

```
AT+MDNSSRVDEREG=Provision,,,_http,_tcp,local
OK
```

```
AT+MDNSSTOP
OK
```

3.12.8 MDNS Services Announce

This command is used to announce the MDNS services.

Command Syntax AT+MDNSANNOUNCE

Synchronous Response

Table 132, page 158 describes the synchronous responses and remarks for the MDNS Services Announce command.

Table 132 MDNS Services Announce Synchronous Responses

Responses	Remarks
OK	Success Prior to issuing this command, the node should start the MDNS module.
ERROR	Failure Before issuing this command, the node is not started with an MDNS module.

Example AT+MDNSACCOUNCE
OK

Example - All MDNS Commands AT+WA=GainSpanDemo,,11
IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK

AT+NDHCP-1
IP SubNet Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK

AT+WEBPROV=admin,admin
OK

AT+MDNSSTART
OK

AT+MDNSHNREG=Prov,local
OK
Registration Success! for RR:Prov
AT+MDNSSRVREG=Provisioning,,_http,_tcp,local,80,0,path=/gsprov.html
OK

Registration Success!! for RR: Provisioning
AT+MDNSANNOUNCE
OK

```
AT+MDNSHNDREG=Prov, local
OK
```

```
AT+MDNSSRVDEREG=Provision,,_http,_tcp,local
OK
```

```
AT+MDNSSTOP
OK
```

3.12.9 MDNS Service Discover

This command is used to discover the MDNS services.

Command Syntax

```
AT+MDNSSD=[<Servicesubtype>],<Servicetype>,<Protocol>,<Do
main>
```

Parameter Description

Table 133, page 159 describes the MDNS Service Discover parameters.

Table 133 MDNS Service Discover Parameters

Parameter	Optional/Mandatory	Value	Description
ServiceSubType	Optional	N/A	<i>ServiceSubType</i> is the name of the service subtype if any.
ServiceType	Optional	N/A	<i>ServiceType</i> is the type of service, for example HTTP, FTP, etc.
Protocol	Mandatory	N/A	<i>Protocol</i> is the protocol used (TCP, UDP).
Domain	Mandatory	N/A	Name of the domain. It should be “ <i>local</i> ”

Synchronous Response

Table 134, page 159 describes the synchronous responses and remarks for the MDNS Service Discover command.

Table 134 MDNS Service Discover Synchronous Responses

Responses	Remarks
OK	Success Prior to issuing this command, the node should start the MDNS module and should register the services.
ERROR:INVALID INPUT	Failure Before issuing this command, the node has not started with the MDNS module.

Example

```
AT+MDNSSD=,_http,_tcp,local
```

3.12.10 MDNS Module De-Initialization

This command is used to stop the MDNS module.

Command Syntax AT+MDNSSTOP

Synchronous Response

Table 135, page 160 describes the synchronous responses and remarks for the MDNS Module De-Initialization command.

Table 135 MDNS Module De-Initialization Synchronous Responses

Responses	Remarks
OK	Success Prior to issuing this command, the node should start the MDNS module.

Example AT+MDNSSTOP
OK

Example - All MDNS Commands AT+WA=GainSpanDemo,,11
IP SubNet Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK

AT+NDHCP-1
IP SubNet Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK

AT+WEBPROV=admin,admin
OK

AT+MDNSSTART
OK

AT+MDNSHNREG=Prov,local
OK

Registration Success! for RR:Prov
AT+MDNSSRVREG=Provisioning,,_http,_tcp,local,80,0,path=/gsprov.html
OK

Registration Success!! for RR: Provisioning
AT+MDNSANNOUCE
OK

```
AT+MDNSHNDREG=Prov, local
OK
```

```
AT+MDNSSRVDEREG=Provision,,_http,_tcp,local
OK
```

```
AT+MDNSSTOP
OK
```

3.12.11 DHCP Server for IPv4

This command is used to start/stop the DHCP server. Prior to starting the server, the adapter should be configured with a valid static IP address (using commands described in [3.12.2 Static Configuration of Network Parameters for IPv4, page 147](#), both Src address and Gateway should be same) and created or configure to create a limited AP network.

This DHCP server can support maximum 32 client connections with server IP as the statically configured IP address and client IP address starts from the next IP address of the configured static IP address.

Command Syntax

```
AT+DHCPSSRVR=<Start/Stop>[,<DnsOptionDisable>,<GatewayOpti
onDisable>]
```

Parameter Description

[Table 136, page 161](#) describes the DHCP Server for IPv4 parameters.

Table 136 DHCP Server for IPv4 Parameters

Parameter	Optional/Mandatory	Value	Description
Start/Stop	Mandatory	0	Stops the server
		1	Starts the Server
DnsOptionDisable	Optional	0 (default)	Enable
		1	Disable
GatewayOptionDisable	Optional	0 (default)	Enable
		1	Disable

Synchronous Response

Table 137, page 162 describes the synchronous responses and remarks for the DHCP Server for IPv4 command.

Table 137 DHCP Server for IPv4 Synchronous Responses

Responses	Remarks
OK	Success The node is statically configured with IP address, and configured to create a limited AP. The client IP address starts from the next IP address of the configured IP address.
ERROR:INVALID INPUT	Failure Enabling DHCP server (AT+DHCPSSVR=1), if the node has already started the DHCP server.

Example

AT+DHCPSSVR=1

OK

AT+DHCPSSVR=1

ERROR

Example Use Case

AT+NSET=192.168.5.1,255.255.255.0,192.168.5.1

OK

AT+WM=2

OK

AT+WA=GainSpanDemo,,11

IP SubNet Gateway

192.168.5.1:255.255.255.0:192.168.5.1

OK

AT+DHCPSSVR=1

OK

3.12.12 DHCP Server Configuration for IPv4

This command is used to configure the DHCP server. It should be issued prior to the DHCP server start command.

Command Syntax AT+DHCP_SRVRCFG=<start_ip_address>,<no_of_clients>

Parameter Description

Table 138, page 163 describes the DHCP Server Configuration parameters.

Table 138 DHCP Server Configuration Parameters

Parameter	Optional/Mandatory	Value	Description
start_ip_address	Mandatory	N/A	The first IP address assigned by the DHCP server when the client requests an IP. Format should be: xxx.xxx.xxx.xxx
no_of_clients	Mandatory	N/A	The number of clients supported by the DHCP server.

Synchronous Response

Table 139, page 163 describes the synchronous responses and remarks for the DHCP Server Configuration command.

Table 139 DHCP Server Configuration Synchronous Responses

Responses	Remarks
OK	Success Command executed.
ERROR	Failure

3.12.13 DNS Server

This command is used start/stop the DNS server. Prior to start the server, the DHCP server should be started and created or configure to create a limited AP network. This DNS server use the same DHCP server IP address as its IP address (see [3.12.3 MDNS Module Initialization for IPv4](#), page 148).

Command Syntax AT+DNS=<Start/stop>,<url>

Parameter Description

Table 140, page 164 describes the DNS Server parameters.

Table 140 DNS Server Parameters

Parameter	Optional/Mandatory	Value	Description
Start/Stop	Mandatory	0	Stops the server
		1	Starts the Server
url	Optional	N/A	URL is the ENS name associated to the DNS IP address.

Synchronous Response

Table 141, page 164 describes the synchronous responses and remarks for the DNS Server command.

Table 141 DNS Server Synchronous Responses

Responses	Remarks
OK	Success The node is statically configured with IP address, and configured to create a limited AP. The client IP address starts from the next IP address of the configured IP address.
ERROR:INVALID INPUT	If the parameters are not valid. (other than 0/1 or url is not)

Example Use Case - Configure the node as a limited AP, start the DNS server

Serial2WiFiAPP
AT+NSET=192.168.7.1,255.255.255.0,192.168.7.1
OK

AT+DHCP_SRV=1
OK

AT+WM=2
OK

AT+WA=GainSpanDemo,,11
IP SubNet Gateway
192.168.7.1:255.255.255.0:192.168.7.1

OK

AT+DNS=1, www.gainspandemo.com
OKAT+WEBPROV=admin, admin
OK

3.12.14 DNS Lookup (Client)

This command is used to receive an IP address from a host name. Upon deployment of this command, the node queries the DNS server to obtain the IP address corresponding to the host name provided in URL, and returns the address if found or ERROR if the URL does not exist.

Command Syntax AT+DNSLOOKUP=<URL>, [<Retry count>, <Retry timeout>]

Command Note If the server does not respond or is not reachable, then the application retries for the specified number of times provided by the optional parameters <Retry count> and <Retry timeout> in the command. The retry count is addition to the first attempt.

Example AT+DNSLOOKUP=www.gainspan.com, 2, 5

Parameter Description

Table 142, page 165 describes the DNS Lookup (Client) parameters.

Table 142 DNS Lookup (Client) Parameters

Parameter	Optional/Mandatory	Value	Description
URL	Mandatory	N/A	URL is the host name to be identified.
Retry count	Optional	1-10 range 3 (default)	It is the number of times node retries to query the URL. This excludes the initial attempt of query. This is applicable for primary and secondary DNS. If value is not given or 0 is provided, then the default value is used.
Retry timeout	Optional	1-20 seconds 5 seconds (default)	It is the time interval between two retries. The node waits for the specified time after sending a query request.

Synchronous Response

Table 143, page 166 describes the synchronous responses and remarks for the DNS Lookup (Client) command.

Table 143 DNS Lookup (Client) Synchronous Responses

Responses	Remarks
IP:<ip address> OK	Success Prior to issuing this command the node should be associated to the network.
ERROR	Failure If the node is not associated before issuing this command (Valid command is executed but DNS lookup fails).
ERROR:INVALID INPUT	Failure If valid command is not executed.

The node returns 0 for OK, and 1 for ERROR if a valid command was issued, but DNS lookup failed (if verbose mode is disabled).

Example

```
AT+NDHCP=1  
OK
```

```
AT+WA=GainSpanDemo,,1  
ERROR
```

```
AT+WA=GainSpanDemo,,11  
IP SubNet Gateway  
192.168.44.110:255.255.255.0:192.168.44.1  
OK
```

```
AT+DNCLOOKUP=www.gainspan.com  
IP:23.23.181.241  
OK
```

3.12.15 Static Configuration of DNS (Client)

This command is used to set the IP address of the DNS server to be used by the node. The second DNS2 IP is optional but should not be the same as DNS1 IP address.

Command Syntax AT+DNSSET=<DNS1 IP>, [<DNS2 IP>]

Command Note This command must be issued before associating to a network. This static configuration of DNS set will take effect only in the case of static IP address on the adapter.

Parameter Description

Table 144, page 167 describes the Static Configuration of DNS (Client) parameters.

Table 144 Static Configuration of DNS (Client) Parameters

Parameter	Optional/Mandatory	Value	Description
DNS1 IP	Mandatory	N/A	<i>DNS1 IP</i> is the IP address of the DNS server.
DNS2 IP	Optional	N/A	<i>DNS2 IP</i> should not be the same as DNS1 IP address.

Synchronous Response

Table 145, page 167 describes the synchronous responses and remarks for the Static Configuration of DNS (Client) command.

Table 145 Static Configuration of DNS (Client) Synchronous Responses

Responses	Remarks
OK	Success To take effect, this command should be given before associating to the network.
ERROR	Failure If the parameters are not valid.

3.12.16 IP Multicast Join

This command is used to join the specified multicast group (specified by the IP address).

Command Syntax AT+NIPMULTICASTJOIN=<Group IP>

Synchronous Response

Table 146, page 168 describes the synchronous responses and remarks for the IP Multicast Join command.

Table 146 IP Multicast Join Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure

3.12.17 IP Multicast Leave

This command is used to leave the specified multicast group (specified by the IP address).

Command Syntax AT+NIPMULTICASTLEAVE=<Group IP>

Synchronous Response

Table 147, page 168 describes the synchronous responses and remarks for the IP Multicast Leave command.

Table 147 IP Multicast Leave Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure

3.12.18 Store Network Context

This command will be used to store the network context and configuration parameters prior to a transition to standby. This command will store the network connection parameters (WiFi layer and network layer information) in RTC memory, when the GainSpan SoC is sent to standby mode using request standby command (see [3.20.3 Request Standby Mode, page 250](#)).

Command Syntax

AT+STORENWCONN

Synchronous Response

[Table 148, page 169](#) describes the synchronous responses and remarks for the Store Network Context command.

Table 148 Store Network Context Synchronous Responses

Responses	Remarks
OK	Success Associate to a network. Upon issue of this command will store the network parameters into the RTC memory.
DISASSOCIATED	Failure If the node is not associated before issuing this command it will display the network context.

3.12.19 Restore Network Context

This command is used to read the IP layer network connection parameters saved by Store Network Context (see [3.12.16 IP Multicast Join, page 168](#)), and reestablishes the connection that existed before the transition to Standby. If needed, the node will re-associate and re-authenticate with the specified SSID. With ARP cache enabled, this command restores the ARP entries stored in the non-volatile memory to the nodes network stack.

Command Syntax

AT+RESTORENWCNN

Synchronous Response

[Table 149, page 170](#) describes the synchronous responses and remarks for the Restore Network Context command.

Table 149 Restore Network Context Synchronous Responses

Responses	Remarks
OK	Success Reads the IP layer network connection parameters saved by “Store Network Context” and reestablishes the connection that existed before the transition to standby.
ERROR	Failure If the command is issued, prior to storing the network connection, or after storing the network connection but before a transition to Standby has occurred.

Example

AT+NDHCP=1

OK

AT+WA=GainSpanDemo,,11

IP SubNet Gateway
192.168.44.110:255.255.255.0:192.168.44.1
OK

AT+STORENWCNN

OK

AT+PSSTBY=10000

Out of Standby-Timer

AT+RESTORENWCNN

OK

3.12.20 ARP Cache Enable

This command is used to enable the cache for ARP entries (maximum 8) in its non-volatile memory and available across standby wakeup cycle. The node starts caching ARP entries and upon the store network command update to its nonvolatile memory (see [3.12.15 Static Configuration of DNS \(Client\), page 167](#)). ARP aging is not supported. When WiFi layer connection is lost, the ARP entries will also be invalidated.

Command Syntax AT+NARPCHACHEEN=<Enable>

Parameter Description

[Table 150, page 171](#) describes the ARP Cache Enable parameters.

Table 150 ARP Cache Enable Parameters

Parameter	Optional/Mandatory	Value	Description
Enable	Mandatory	1 - Enable (Default value)	Start caching
		0 - Disable	Stop caching

Synchronous Response

[Table 151, page 171](#) describes the synchronous responses and remarks for the ARP Cache Enable command.

Table 151 ARP Cache Enable Synchronous Responses

Responses	Remarks
OK	Success Prior to issuing this command the node should be associated to the network.
ERROR:INVALID INPUT	Failure If the parameters are not valid. (value other than 0 or 1)

Example

```
AT+WA=GainSpanDemo,,1
IP           SubNet        Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK
```

```
AT+NDHCP=1
IP           SubNet        Gateway
192.168.44.145:255.255.255.0:192.168.44.1
OK
```

```
AT+NARPCHACHEEN=1
OK
```

3.12.21 ARP Entry Listing

This command is used to list all ARP entries present in the nodes network stack.

Command Syntax AT+NARP=?

Synchronous Response

Table 152, page 172 describes the synchronous responses and remarks for the ARP Entry Listing command.

Table 152 ARP Entry Listing Synchronous Responses

Responses	Remarks
Macaddress:IP address	Success
OK	Displays the ARP entries present in the nodes network stack. The MAC address is in the format xx:xx:xx:xx:xx:xx and the IP address is in the format xx:xx:xx:xx:xx:xx.
OK	If no ARP entries present.

Example

```
AT+NARP=?
c8:d7:19:75:74:f9:192.168.44.1
60:67:20:3f:10:e0:192.168.44.144
OK
```

3.12.22 ARP Entry Set

This command is used to set a static entry in the ARP table.

Command Syntax AT+NARPSET=<Ip address>,<Mac address>

Command Note This command must be issued after associating to a network.

Parameter Description

Table 153, page 173 describes the ARP Entry Set parameters.

Table 153 ARP Entry Set Parameters

Parameter	Optional/Mandatory	Description
Ip address	Mandatory	xxxx.xxxx.xxxx.xxxx format.
Mac address	Mandatory	xx:xx:xx:xx:xx:xx format.

Synchronous Response

Table 154, page 173 describes the synchronous responses and remarks for the ARP Entry Set command.

Table 154 ARP Entry Set Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure

3.12.23 ARP Entry Delete

This command is used to delete an entry in the ARP table.

Command Syntax AT+NARPDELETE=<Ip address>,<Mac address>

Command Note This command must be issued after associating to a network.

Parameter Description

Table 155, page 174 describes the ARP Entry Delete parameters.

Table 155 ARP Entry Delete Parameters

Parameter	Optional/Mandatory	Description
Ip address	Mandatory	xxxx.xxxx.xxxx.xxxx format.
Mac address	Mandatory	xx:xx:xx:xx:xx:xx format.

Synchronous Response

Table 156, page 174 describes the synchronous responses and remarks for the ARP Entry Delete command.

Table 156 ARP Entry Delete Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure

3.12.24 ARP Learning

This command is used to enable or disable updating ARP entries to network stack.

When ARP learning is enabled, the ARP table is updated based on the application filter and the ARP request packets received. Currently, the default application filter drops all the ARP request packets which are not destined to the GS2000 node. Therefore, learning is only from the incoming ARP request packets for the node.



NOTE: There is no AT command to change or update this behavior in the S2W default filter. There are only AT commands to change the UDP/TCP receive behaviors in the S2W default filter.

When ARP learning is disabled, the ARP table is updated only when the ARP request is sent from the GS2000 and the ARP response is received for the same. The ARP table is not updated in any other case.

Command Syntax

AT+NARPAUTO=n

Command Note

This command must be issued after associating to a network.

Table 157, page 175 describes the parameter in ARP Learning command.

Table 157 ARP Learning Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0: Enable 1: Disable Default value: 1	When ARP Learning is enabled, ARP cache is updated with the entry based on ARP response information. When ARP learning is disabled, the ARP table is updated only when the ARP request is sent from the GS2000 and the ARP response is received for the same.

Synchronous Response

Table 158, page 175 describes the synchronous responses and remarks for the ARP Learning command.

Table 158 ARP Learning Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure - When the parameter is other than 0 or 1.

3.12.25 Gratuitous ARP

This command is used to send gratuitous ARP.

Command Syntax AT+GRATARP

Synchronous Response

[Table 158, page 175](#) describes the synchronous responses and remarks for the ARP Learning command.

Table 159 Gratuitous ARP Synchronous Responses

Responses	Remarks
OK	Success
ERROR: INVALID INPUT	If the command is provided with any input values. Example: AT+GRATARP=0.

3.13 Connection Management Configuration

All connection commands, except for the transport of Raw Ethernet data (see [3.13.18 HTTP Client Close, page 212](#)), use the embedded TCP/IP Network Stack functions to perform the required actions. Connection identifiers, denoted as <CID> below, are to be sent as single hexadecimal characters in ASCII format.

3.13.1 Network Interface Filter

This command supports the S2W adapter feature called network interface filter, which controls the traffic to the network stack so that unwanted TCP/UDP/ICMP packets can be dropped before giving to the network stack. This feature prevents the DOS attacks.

Command Syntax AT+L2CONFIG=<Protocol>,<Enable/Disable>

Command Note GainSpan node supports a feature called network interface filter which controls the traffic to the network stack so that unwanted TCP/UDP/ICMP packets can be dropped before giving to the network stack. This feature prevents the DOS attacks.

Parameter Description

[Table 160, page 177](#) describes the Network Interface Filter parameters.

Table 160 Network Interface Filter Parameters

Parameter	Optional/Mandatory	Value	Description
Protocol	Mandatory	1	For ICMP
		2	For UDP and TCP
		Parameter is configured as a bit wise.	
Enable/Disable	Mandatory	0 (default)	For Disable
		1	For Enable
		Parameter is configured as bit wise.	

Synchronous Response

[Table 161, page 177](#) describes the synchronous responses and remarks for the Network Interface Filter command.

Table 161 Network Interface Filter Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Failure If the parameters are not valid.

Example 1 - Enables the filter for ICMP reception So that no ICMP packets will not go to network stack.
AT+L2CONFIG=1, 1
OK

Example 2 - Disables the above command AT+L2CONFIG=1, 0
OK

Example 3 - Enables the filter for UDP and TCP reception So that no UDP/TCP packets with an invalid port will not go to the network stack.
AT+L2CONFIG=2, 2
OK

Example 4 - Disables the command above AT+L2CONFIG=2, 0
OK

Example 5 - Enables the filter for ICMP/UDP and TCP AT+L2CONFIG=3, 3
OK

Example 6 - Disables the command AT+L2CONFIG=3, 0
OK

Example Use Case GainSpan node is configured as a TCP server and enabled network interface filter with Server IP: 9003 and I2config for UDP/TCP enabled.

```
AT+WA=GainSpanDemo,,11
IP           SubNet          Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK
```

```
AT+NSTCP=9003
CONNECT0
OK
```

```
AT+L2CONFIG=2, 2
OK
```

3.13.2 Get Network Interface Filter Configuration

This command is used to get the configured current network interface filter.

Command Syntax AT+L2CONFIG=?

Synchronous Response

Table 162, page 179 describes the synchronous responses and remarks for the Get Network Interface Filter Configuration command.

Table 162 Get Network Interface Filter Configuration Synchronous Responses

Responses	Remarks
CONFIG MAP:<value> OK	<i>value</i> is the configured network interface filter.

Example
AT+L2CONFIG=1,1
OK

AT+L2CONFIG=?
CONFIG MAP:01
OK

3.13.3 TCP Clients for IPv4

This command is used to create a TCP client connection to the remote server with IPv4 address.



NOTE: If the receiving TCP is unable to consume data and the host keeps transmitting TCP data, then there is a possibility that the receiver may reach zero window. As the host keeps transmitting TCP data, the data is accumulated in GS network stack. In such cases, processing the next TCP data send (from host) would be blocked causing the serial interface to be blocked.
This condition will be cleared when the receiver updates its window or the TCP timeout happens for the data that is stored in GS network stack.

Command Syntax AT+NCTCP=<Dest-Address>, <Port>

Parameter Description

Table 163, page 180 describes the TCP Clients for IPv4 parameters.

Table 163 TCP Clients for IPv4 Parameters

Parameter	Optional/Mandatory	Value	Description
Dest-Address	Mandatory	N/A	Dest-Address is the destination (server) IP address.
Port	Mandatory	N/A	Port is the destination (server) port.

Synchronous Response

Table 164, page 181 describes the synchronous responses and remarks for the TCP Clients for IPv4 command.

Table 164 TCP Clients for IPv4 Synchronous Responses

Responses	Remarks
CONNECT <CID> OK	Success
ERROR	Upon connection failure or invalid parameter.
ERROR: NO CID	GS node supports only 16 clients, it will not create the next connection (i.e., 17th connection) when all 16 connections (CIDs) are being active.

Asynchronous Response

Table 165, page 181 describes the asynchronous responses and remarks for the TCP Clients for IPv4 command.

Table 165 TCP Clients for IPv4 Asynchronous Responses

Responses	Remarks
DISCONNECT <CID>	TCP connection with the given CID is closed. This response is sent to the host when a connection is closed by the remote server.
ERROR: SOCKET FAILURE <CID>	Upon connection failure.

Example Use Case GainSpan (GS) node is configured as a TCP client with:

```

Server IP: 192.168.23.100
Server port: 3009

AT+WA=GainSpanDemo
IP           SubNet        Gateway
192.168.1.99:255.255.255.0:192.168.1.1
OK

AT+NDHCP=1
IP           SubNet        Gateway
192.168.17.3:255.255.255.0:192.168.17.1
OK

AT+NCTCP=192.168.23.100,3009
CONNECT 0
OK
  
```

Example Use Case When AT+NCTCP is executed before L2/L3:

```
Serial2WiFiAPP
AT+NCTCP=192.168.12.1,1234
DISASSOCIATED
OK

AT+WSTATUS
NOT ASSOCIATED
OK

AT+NSTAT=?
MAC=00:1d:c9:1b:93:b0
WSTATE=NOT CONNECTED MODE=NONE
BSSID=00:00:00:00:00:00 SSID="" CHANNEL=NONE SECURITY=NONE
RSSI=0
IP addr=0.0.0 SubNet=0.0.0.0 Gateway=0.0.0.0
DNS1=0.0.0.0 DNS2=0.0.0.0
Rx Count=0 Tx Count=0
OK

AT+CID=?
No Valid Cids
OK
```

3.13.4 UDP Clients for IPv4

This command is used to open a UDP client connection to the remote sever with IPv4 address. Upon deployment of this command, the interface opens a UDP socket capable of sending data to the specified destination address and port.



NOTE: GS node receives UDP packets of size less than or equal to 1500 bytes.

Command Syntax

AT+NCUDP=<Dest-Address>,<Port>[<,Src.Port>]

Parameter Description

Table 166, page 183 describes the UDP Clients IPv4 parameters.

Table 166 UDP Clients IPv4 Parameters

Parameter	Optional/Mandatory	Value	Description
Dest-Address	Mandatory	N/A	Dest-Address is the destination (server) IP address.
Dest-Port	Mandatory	N/A	Port is the destination (server) port.
Src-Port	Optional	N/A	Port is the source (client) port. If a source port is provided, the socket will bind to the specified port.

Synchronous Response

Table 167, page 183 describes the synchronous responses and remarks for the UDP Clients IPv4 command.

Table 167 UDP Clients IPv4 Synchronous Responses

Responses	Remarks
CONNECT <CID> OK	Successful connection
ERROR: SOCKET FAILURE <CID>	When the active Src-Port and the active Dest-Port number is being used for creating new connections.
ERROR: NO CID	GS node support only 16 CIDs, it will not create the next connection (i.e., 17 th connection) when all 16 CIDs are being active.

Example Use Case

GainSpan (GS) node is configured as a UDP client with:

```
Server IP: 192.168.23.100
Server port: 9003
```

```
AT+WA=GainSpanDemo
IP           SubNet          Gateway
192.168.1.99:255.255.255.0:192.168.1.1
```

OK

```
AT+NDHCP=1
IP           SubNet        Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK
```

```
AT+NCUDP=192.168.23.100,9003
CONNECT 0
OK
```

Command Note The port range 0xBAC0(47808) to 0xBACF (47823) may not be used for destination port.

3.13.5 TCP Servers for IPv4

This command is used to start the TCP server connection with IPv4 address.



NOTE: If the receiving TCP is unable to consume data and the host keeps transmitting TCP data, then there is a possibility that the receiver may reach zero window. As the host keeps transmitting TCP data, the data is accumulated in GS network stack. In such cases, processing the next TCP data send (from host) would be blocked causing the serial interface to be blocked.
This condition will be cleared when the receiver updates its window or the TCP timeout happens for the data that is stored in GS network stack.

Command Syntax AT+NSTCP=<Port>, [max client connection]

Parameter Description

Table 168, page 184 describes the TCP Servers for IPv4 parameters.

Table 168 TCP Servers for IPv4 Parameters

Parameter	Optional/Mandatory	Value	Description
Port	Mandatory	N/A	The interface opens a socket on the specified port and listens for connections.

Synchronous Response

Table 169, page 185 describes the synchronous responses and remarks for the TCP Servers for IPv4 command.

Table 169 TCP Servers for IPv4 Synchronous Responses

Responses	Remarks
CONNECT <CID> OK Example: CONNECT 0	Success TCP connection successful. <CID> = the new CID in hexadecimal format.
CONNECT <SERVER_ID> <CLIENT_ID> <CLIENT_IP> <CLIENT_PORT> Example: CONNECT 0 1 192.168.17.2 50569 Where, 0 - server_cid 1 - client_cid 192.168.23.100 - client_ip 50569 - client_port	Success Successful connection establishment of TCP client (Hercules) to GS node (TCP server).
DISCONNECT <CID> Example: DISCONNECT 1	Client disconnects the connection from GS node (TCP server).
ERROR:NO CID	GS node supports 16 CIDs, when 16 connections are established and tries to connect for 17 th connection, then an error message will be displayed for insufficient memory.
ERROR:SOCKET FAILURE <CID> Example: ERROR: SOCKET FAILURE 0	When the same port is used for creating TCP sever, then GS node displays an error message for the duplicate port.

Asynchronous Response

Table 170, page 185 describes the asynchronous responses and remarks for the TCP Servers for IPv4 command.

Table 170 TCP Servers for IPv4 Asynchronous Responses

Responses	Remarks
CONNECT <SERVER_ID> <CLIENT_ID> <CLIENT_IP> <CLIENT_PORT>	When client (TCP client) connects to GS node (TCP server).
DISCONNECT <CID> Example: DISCONNECT 3	TCP connection with the given CID is closed. This response is sent to the host when a connection is closed by the remote device (TCP client).

Example Use Case GainSpan (GS) node is configured as a TCP server with,
Port: 8005

```
AT+NDHCP=1
OK

AT+WA=GainSpanDemo,,11
IP SubNet Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK

AT+NSTCP=8005
CONNECT 0
```

Example Use Case When AT+NSTCP is executed before L2/L3:

```
Serial2WiFiAPP
AT+NCTCP=192.168.12.1,1234
DISASSOCIATED
OK

AT+NSTCP=3456
DISASSOCIATED

AT+NSTCP=8888
DISASSOCIATED

AT+WSTATUS
NOT ASSOCIATED
OK

AT+NSTAT=?
MAC=00:1d:c9:1b:93:b0
WSTATE=NOT CONNECTED MODE=NONE
BSSID=00:00:00:00:00:00 SSID="" CHANNEL=NONE SECURITY=NONE
RSSI=0
IP addr=0.0.0 SubNet=0.0.0.0 Gateway=0.0.0.0
DNS1=0.0.0.0 DNS2=0.0.0.0
Rx Count=0 Tx Count=0
OK

AT+NSTCP=1234
DISASSOCIATED

AT+CID=?
No Valid Cids
OK
```

3.13.6 UDP Servers for IPv4

This command is used issued to start a UDP server connection with IPv4 address.



NOTE: GS node receives UDP packets of size less than or equal to 1500 bytes.

Command Syntax

AT+NSUDP=<Port>

Parameter Description

Table 171, page 187 describes the UDP Servers IPv4 parameters.

Table 171 UDP Servers IPv4 Parameters

Parameter	Optional/Mandatory	Value	Description
Port	Mandatory	N/A	Server port (The port range 0xBAC0 (47808) to 0xBACF (47823) may not be used).

Synchronous Response

Table 172, page 187 describes the synchronous responses and remarks for the UDP Servers IPv4 command.

Table 172 UDP Servers IPv4 Synchronous Responses

Responses	Remarks
CONNECT <CID>	Success
OK	UDP connection successful. <i>cid</i> is the new connection id in hexadecimal format.
Example: CONNECT 0	
ERROR:SOCKET FAILURE <CID>	When the same port is used for creating UDP server, then GS node displays an error message for the duplicate port.
Example: ERROR: SOCKET FAILURE 0	
ERROR:NO CID	GS node supports 16 CIDs, when 16 connections are established and tries to connect for 17th connection, then an error message will be displayed.

Example Use Case GainSpan (GS) node is configured as a UDP server with port 1009.

```
AT+NDHCP=1
OK

AT+WA=GainSpanDemo,,11
IP           SubNet          Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK

AT+NSUDP=1009
CONNECT 0
OK
```

3.13.7 Connection Status

This command is used to return the current CID configuration for all existing CIDs.

Command Syntax AT+CID=?

Usage This command returns the current CID configuration for all existing CIDs:

1. CID number (in decimal format)
2. CID type
3. Mode
4. Local port
5. Remote port
6. Remote IP address

Synchronous Response

Table 173, page 189 describes the synchronous responses and remarks for the Output Connections command.

Table 173 Output Connections Synchronous Responses

Responses	Remarks
<CID> <TYPE <MODE> <LOCALPORT> <REMOTE PORT> <REMOTE IP> OK	If valid CIDs are present
No valid CIDs	If no valid CIDs are present.

Example

```
AT+CID=?
```

CID	TYPE	MODE	LOCAL PORT	REMOTE PORT	REMOTE IP
0	UDP	SERVER	1009	0	0.0.0.0
1	UDP	CLIENT	46445	9001	192.168.23.100
5	TCP	CLIENT	62771	9007	192.168.23.100
6	TCP	SERVER	4000	0	0.0.0.0
3	TCP-SSL	CLIENT	44499	443	192.168.2.73

```
OK
```

3.13.8 Closing a Connection

This command is used to close the connection associated with the specified CID, if it is currently open. On completion of this command the CID is free for use in future connections.

Command Syntax AT+NCLOSE=<CID>

Parameter Description

Table 174, page 191 describes the Closing a Connection parameters.

Table 174 Closing a Connection Parameters

Parameter	Optional/Mandatory	Value	Description
CID	Mandatory	16 (maximum)	CID is the allocated connection identifier.

Synchronous Response

Table 175, page 191 describes the synchronous responses and remarks for Closing a Connection command.

Table 175 Closing a Connection Synchronous Responses

Responses	Remarks
OK	Connection with the given CID is closed, and this CID can be used for future connection.
INVALID CID	If any invalid CID is provided.

Example Use Case GainSpan (GS) node is configured with the TCP client connection and closed the connection using “nclose.”

```
AT+NDHCP=1
OK
```

```
AT+WA=GainSpanDemo,,11
IP           SubNet          Gateway
192.168.23.101:255.255.255.0,192.168.23.1
OK
```

```
AT+NCUDP=192.168.23.100,8005
CONNECT 8
OK
```

```
AT+NCLOSE=8
OK
```

3.13.9 Closing All Connections

This command is used to close all open connections.

Command Syntax AT+NCLOSEALL

Synchronous Response

Table 176, page 192 describes the synchronous responses and remarks for Closing All Connections command.

Table 176 Closing All Connections Synchronous Responses

Responses	Remarks
OK	All open connections are closed.

Example AT+NCLOSEALL
OK

3.13.10 Socket Options Configuration

This command is used to configure a socket which is identified by a CID.

Command Syntax AT+NXSETSOCKOPT=<CID>,<Type>,<Parameter>,<Value>,<Length>

Parameter Description

Table 177, page 192 describes the Socket Options Configuration parameters.

Table 177 Socket Options Configuration Parameters

Parameter	Optional/Mandatory	Value	Type/Name	Description
CID	Mandatory	16 (maximum) connection identifiers are allowed.	N/A	CID is the socket identifier received after opening a connection.
Type	Mandatory	1	SOL_SOCKET	It specifies the category type for Socket.
		3	IP_PROTOTCP	It specifies the category type for TCP.

Table 177 Socket Options Configuration Parameters (Continued)

Parameter	Optional/Mandatory	Value	Type/Name	Description
Parameter	Mandatory	29	TCP_MAXRT	It specifies the maximum retransmission timeout in seconds.
		9	TCP_KEEPALIVE	It allows to enable or disable sending keep alive packets after the predefined time of 30 seconds.
		2A	TCP_MAX_REXMIT	It specifies the maximum number of retransmission count.
		2B	TCP_REX_TIMER_RATE	It is used to set the retransmission timer rate.
		8	SO_RCVBUF	It sets the receive buffer size for TCP packets. The maximum limit is 64KB.
		2E	TCP_MAX_TX_Q_DEPTH	It specifies the TCP transmission queue depth in terms of number of packets.
		2F	TCP_REX_TIMER_RATE_IN_NW_TICKS	It specifies the transmission rate in terms of network ticks.

Table 177 Socket Options Configuration Parameters (Continued)

Parameter	Optional/Mandatory	Value	Type/Name	Description
Note: The following NXSETSOCKOPTs are not supported in network stack. <ul style="list-style-type: none"> • SO_SENDBUF • SO_RESUSEPORT • Enabling or disabling Nagle algorithm. It is disabled by default in the network stack. 				
Value	Mandatory	• •	N/A	<ul style="list-style-type: none"> • For retransmission timeout, the <i>value</i> is time to be set in terms of seconds. • For retransmission count, the <i>value</i> is a number. Once the number of retransmissions for a packet reaches this value, the socket is automatically closed by the network stack. • For retransmission timer rate, the <i>value</i> is time to be set in terms of seconds. • For Keepalive, the <i>value</i> to be set is 0 or 1. 1 is to enable Keepalive and 0 is to disable Keepalive. • For buffer, the <i>value</i> is the size of buffer to be set in bytes.
Length	Mandatory	N/A	N/A	It specifies the length of the value in bytes. 4 - Integer 2 - Short 1 - Char

Synchronous Response

Table 178, page 194 describes the synchronous responses and remarks for Socket Options Configuration command.

Table 178 Socket Options Configuration Synchronous Responses

Responses	Remarks
OK	Success
ERROR: SOCKET FAILURE 0	If parameters are not valid.

Example Use Case 1 Enable TCP_KEEPALIVE

GS node and TCP server running on a Host are both connected to an Access Point. Open a TCP client on GS node and check whether the TCP connection between the client and server is idle. If connection is idle, then TCP client (GS node) sends TCP_KEEPALIVE packets every 30 seconds which is the default Keepalive timeout.

To enable TCP_KEEPALIVE, use the following command:

```
AT+NXSETSOCKOPT=1,1,9,0,4
```

Where:

CID - 1

Type - 1 (SOL_SOCKET)

Parameter - 9 (TCP_KEEPALIVE)

Value - 1 (TCP_KEEPALIVE is enabled)

Length - 4 bytes (Integer)



NOTE: TCP_KEEPALIVE timeout can only be enabled or disabled, with a timeout of 30 seconds.

Example Use Case 2 Set the maximum TCP retransmission time (TCP_MAXRT) to 100 seconds.

The maximum retransmission time is set to 25 seconds by default in S2W application with a retransmission interval of 2 seconds.

To configure the retransmission time to 100 seconds, use the following command:

```
AT+NXSETSOCKOPT=1,3,29,100,4
```

Where:

CID - 1

Type - 3 (IP_PROTOTCP)

Parameter - 29 (TCP_MAXRT)

Value - 100 (TCP_MAXRT is set to 100 seconds)

Length - 4 bytes (Integer)

Example Use Case 3 Set the maximum TCP retransmission count (TCP_MAX_REXMIT) to 40.

The maximum retransmission count is set to 12 by default in S2W application with a retransmission interval of 2 seconds.

To configure the retransmission count to 40, use the following command:

```
AT+NXSETSOCKOPT=1, 3, 2A, 40, 4
```

Where:

CID - 1

Type - 3 (IP_PROTOTCP)

Parameter - 2A (TCP_MAX_REXMIT)

Value - 40 (TCP_MAX_REXMIT is set to 40)

Length - 4 bytes (Integer)

Example Use Case 4 Set the retransmission timer rate (TCP_REX_TIMER_RATE) to 1 second.

To configure the retransmission timer rate to 1 second, use the following command:

```
AT+NXSETSOCKOPT=1, 3, 2B, 1, 4
```

Where:

CID - 1

Type - 3 (IP_PROTOTCP)

Parameter - 2B (TCP_REX_TIMER_RATE)

Value - 1 (TCP_REX_TIMER_RATE is set to 1 second)

Length - 4 bytes (Integer)

Example Use Case 5 Set the receive buffer size (SO_RCVBUF) to 4k.

To configure the buffer size to 4k, use the following command:

```
AT+NXSETSOCKOPT=0, 1, 8, 4096, 4
```

Where:

CID - 0

Type - 1 (SOL_SOCKET)

Parameter - 8 (SO_RCVBUF)

Value - 4096 (SO_RCVBUF is set to 4k)

Length - 4 bytes (Integer)

3.13.11 SSL Connection Open

This command is used to open an SSL connection over the TCP connection identified by the CID. For this SSL connection, the adapter uses the certificate stored in memory that is identified by the certificate name. Prior issuing this command, a valid TCP connection should exist with connection identifier as CID.

The client certificate name and client key name are required for SSL client authentication.



NOTE:

- a> Certificates and Key must be in DER format.
- b> If the size of Server key is more than 2k, then GS node as SSL Client will not connect to the SSL Server.

Command Syntax

```
AT+SSLOPEN=<CID>, [<certificate name>, <client certificate name>,<client key name>]
```

Parameter Description

Table 179, page 197 describes the SSL Connection Open parameters.

Table 179 SSL Connection Open Parameters

Parameter	Optional/Mandatory	Value	Description
CID	Mandatory	16 (maximum)	CID is the allocated connection identifier.
certificate name	Optional	N/A	Name of the SSL certificate.
client certificate name	Optional	N/A	Name of the SSL client certificate.
client key name	Optional	N/A	Name of the SSL client key.

Synchronous Response

Table 180, page 197 describes the synchronous responses and remarks for SSL Connection Open command.

Table 180 SSL Connection Open Synchronous Responses

Responses	Remarks
OK	Success

Example

```
AT+NDHCP=1
OK
AT+WA=GainSpanDemo,,11
IP           SubNet          Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK
AT+SETTIME=11/30/2013,11:03:00
OK
AT+NCTCP=192.168.2.73,443
CONNECT 0
OK
AT+SSLOPEN=0
OK
```

3.13.12 SSL Connection Close

This command is used to close the existing SSL connection over the TCP connection identified by the CID.

Command Syntax AT+SSLCLOSE=<CID>

Parameter Description

Table 181, page 198 describes the Closing SSL Connection parameters.

Table 181 Closing SSL Connection Parameters

Parameter	Optional/Mandatory	Value	Description
CID	Mandatory	N/A	CID is the socket identifier received after opening a connection.

Synchronous Response

Table 182, page 198 describes the synchronous responses and remarks for Closing SSL Connection command.

Table 182 Closing SSL Connection Synchronous Responses

Responses	Remarks
OK	Success
ERROR: INVALID CID	Displays error message for invalid connection identifier.

Example

```
AT+NDHCP=1
OK

AT+WA=GainSpanDemo,,11
IP           SubNet       Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK

AT+SETTIME=11/30/2013,11:03:00
OK

AT+NCTCP=192.168.2.73,443
CONNECT 0
OK

AT+SSLOPEN=0
OK

AT+SSLCLOSE=0
OK
```

3.13.13 SSL Configuration

This command is used to configure the SSL parameters.

It supports to configure:

- Domain name check and configure the size of SSL buffer in bytes which is used to store the alternate names (domain names) provided in the incoming server certificate.
- Close an existing SSL connection and configure the timeout value to close the SSL connection.

Command Syntax

AT+SSLCONF=<Configuration ID>,<Configuration value>

Parameter Description

Table 181, page 198 describes the SSL configuration parameters.

Table 183 Configuring SSL Parameters

Parameter	Optional/Mandatory	Value	Description
Configuration ID	Mandatory	1: Domain name check 2: SSL close timeout check	When this parameter is set to 1, GS module performs the domain name check. When this parameter is set to 2, GS module supports . Timeout value is configured using the Configuration value.
Configuration value	Mandatory	Buffer size: up to 2000 bytes Note: Greater than this value depends on the memory availability in GS module.	This configuration value is used when <i>Configuration ID</i> is set to 1. It specifies the buffer size in bytes to store the alternate names (domain names) provided in the incoming server certificate.
Configuration value	Mandatory	Timeout value: 1 to 60 seconds	This configuration value is used when <i>Configuration ID</i> is set to 2. It

Synchronous Response

Table 182, page 198 describes the synchronous responses and remarks for Closing SSL Connection command.

Table 184 Configuring SSL Synchronous Responses

Responses	Remarks
OK	Success
ERROR: INVALID INPUT	If parameters are not valid.

3.13.14 HTTP Configuration

This command is used to configure the HTTP parameters.

Command Syntax

AT+HTTPCONF=<Param>,<Value>

Parameter Description

Table 185, page 201 describes the HTTP Client Configuration parameters.

Table 185 HTTP Client Configuration Parameters

Parameter	Optional/Mandatory	Description
Param	Mandatory	<p><i>Param</i> is the HTTP header. Custom header starts from 255 onwards and any standard header should start before this. The HTTP header is one of the following.</p> <p>GSN_HTTP_HEADER_AUTHORIZATION (2) GSN_HTTP_HEADER_CONNECTION (3) GSN_HTTP_HEADER_CONTENT_ENCODING (4) GSN_HTTP_HEADER_CONTENT_LENGTH (5) GSN_HTTP_HEADER_CONTENT_RANGE (6) GSN_HTTP_HEADER_CONTENT_TYPE (7) GSN_HTTP_HEADER_DATE (8) GSN_HTTP_HEADER_EXPIRES (9) GSN_HTTP_HEADER_FROM (10) GSN_HTTP_HEADER_HOST (11) GSN_HTTP_HEADER_IF_MODIFIED_SINCE (12) GSN_HTTP_HEADER_LAST_MODIFIED (13) GSN_HTTP_HEADER_LOCATION (14) GSN_HTTP_HEADER_PRAGMA (15) GSN_HTTP_HEADER_RANGE (16) GSN_HTTP_HEADER_REFERER (17) GSN_HTTP_HEADER_SERVER (18) GSN_HTTP_HEADER_TRANSFER_ENCODING (19) GSN_HTTP_HEADER_USER_AGENT (20) GSN_HTTP_HEADER_WWW_AUTHENTICATE (21) GSN_HTTP_REQUEST_URL (23) S2W_HTTPC_CFG_PARAM_CLOSE_TIMEOUT(27)</p>
Value	Mandatory	<i>Value</i> is the string that depends on the above parameter. When <i>param</i> is 11 (GSN_HTTP_HEADER_HOST), then the <i>value</i> string will be 192.168.2.73 (Host address)

Synchronous Response

Table 186, page 202 describes the synchronous responses and remarks for HTTP Client Configuration command.

Table 186 HTTP Client Configuration Synchronous Responses

Responses	Remarks
OK	Success Successful HTTP connection
ERROR: INVALID INPUT	Failure If parameters are not valid.

Example 1

The GainSpan (GS) node (HTTP client) is configured with HTTP header parameters and the HTTP connection is opened with the HTTP server.

Where,

HTTP header configurations are:

3,11,23,2,258 (Added custom header)

```
AT+WA=GainSpanDemo,,11
IP           SubNet       Gateway
192.168.23.101:255.255.255.0:192.168.23.1
OK

AT+HTTPCONF=3,KEEP-ALIVE
OK

AT+HTTPCONF=11,192.168.2.73
OK

AT+HTTPCONF=23,192.168.2.73:443
OK

AT+HTTPCONF=2,Basic dGVzdDp0ZXN0MTIz=test:test123
OK

AT+HTTPCONF=255,SSID:GainSpanDemo
OK

AT+HTTPCONF=256,Temperature:28
OK

AT+HTTPCONF=257,Light:35
OK

AT+HTTPCONF=258,Voltage:3.3
OK

AT+HTTPOPEN=192.168.2.73,80
```

0
OK

Example 2 To configure HTTP close timeout, execute the following command:

AT+HTTPCONF=27,100

Where,

27: S2W_HTTPC_CFG_PARAM_CLOSE_TIMEOUT (27)
100: Timeout value for HTTP close

On successful execution, OK is displayed.

Example 3 To configure HTTP close timeout, execute the following command:

AT+HTTPCONF=27,0
ERROR: INVALID INPUT

An error is displayed as zero is an invalid input value for timeout. The minimum timeout value supported is 10 milliseconds.

3.13.15 HTTP Client Configuration Clear

This command is used to remove an HTTP client configuration.

Command Syntax AT+HTTPCONFDEL=<Param>

Parameter Description

Table 187, page 204 describes the HTTP Client Configuration Removal parameters.

Table 187 HTTP Client Configuration Removal Parameters

Parameter	Optional/Mandatory	Description
Param	Mandatory	GS node removes the HTTP configuration specified by the <i>param</i> . <i>param</i> is the HTTP header and is one of the following. GSN_HTTP_HEADER_AUTHORIZATION (2) GSN_HTTP_HEADER_CONNECTION (3) GSN_HTTP_HEADER_CONTENT_ENCODING (4) GSN_HTTP_HEADER_CONTENT_LENGTH (5) GSN_HTTP_HEADER_CONTENT_RANGE (6) GSN_HTTP_HEADER_CONTENT_TYPE (7) GSN_HTTP_HEADER_DATE (8) GSN_HTTP_HEADER_EXPIRES (9) GSN_HTTP_HEADER_FROM (10) GSN_HTTP_HEADER_HOST (11) GSN_HTTP_HEADER_IF_MODIFIED_SINCE (12) GSN_HTTP_HEADER_LAST_MODIFIED (13) GSN_HTTP_HEADER_LOCATION (14) GSN_HTTP_HEADER_PRAGMA (15) GSN_HTTP_HEADER_RANGE (16) GSN_HTTP_HEADER_REFERER (17) GSN_HTTP_HEADER_SERVER (18) GSN_HTTP_HEADER_TRANSFER_ENCODING (19) GSN_HTTP_HEADER_USER_AGENT (20) GSN_HTTP_HEADER_WWW_AUTHENTICATE (21) GSN_HTTP_REQUEST_URL (23)

Synchronous Response

Table 188, page 205 describes the synchronous responses and remarks for HTTP Client Configuration Removal command.

Table 188 HTTP Client Configuration Removal Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Trying to delete a header parameter which is not configured.
ERROR: INVALID INPUT	Invalid parameter

3.13.16 HTTP Client Connection Open

This command is used to open an HTTP client connection on the GS node to the server specified by the host name and IP address.

Command Syntax

```
AT+HTTPOPEN=<host>[,<Port  
Number>,<SSLFlag>,<CertificateName>,<Proxy>,<Connection  
Timeout>,<ClientCertificateName>,<ClientKeyName>]
```

Parameter Description

Table 189, page 205 describes the HTTP Client Connection Open parameters.

Table 189 HTTP Client Connection Open Parameters

Parameter	Optional/Mandatory	Value	Description
Host	Mandatory	N/A	The host is either the Fully Qualified Domain name (FQDN) of the server or the IP address of the server to which the HTTP client will open the connection (e.g., www.gainspan.com or 74.208.130.221)
PortNumber	Optional	N/A	Port number of the server to which the HTTP client will open the connection. The client can specify the port when the server is running on a non-standard port. Default is the standard port - 80 for HTTP and 443 for HTTPS.
SSLFlag	Optional	0 (default)	SSL Disabled
		1	SSL Enabled
CertificateName	Optional	N/A	The name of the CA Certificate to be used for Server Certificate Authentication in case SSL is enabled. The CA Certificate must be provisioned before this. It uses the certificate configuration on the GS node identified by the certificate name.

Table 189 HTTP Client Connection Open Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
Proxy	Optional	N/A	This flag is used only during HTTPS connection through proxy 1 - The HTTPS connection is through proxy server.
ConnectionTimeout	Optional	N/A	This parameter provides the maximum time limit for setting up of the connection with the server.
ClientCertificateName	Optional	N/A	The client certificate name is required for SSL client authentication and must be provisioned before using this parameter.
ClienKeyName	Optional	N/A	The client key name is required for SSL client authentication and must be provisioned before using this parameter.

Note: Certificates and Key must be in DER format (To add certificate to the GS node use the AT+TCERTADD command (see [3.11.10 EAP Time Validation, page 127](#)).

Synchronous Response

[Table 190, page 206](#) describes the synchronous responses and remarks for HTTP Client Connection Open command.

Table 190 HTTP Client Connection Open Synchronous Responses

Responses	Remarks
<CID> OK	Success
ERROR	Failure If parameters are not valid or if the command is issued before associating to the network.

Example

```
AT+HTTPOPEN=192.168.2.73
1
OK
```

3.13.16.1 Open HTTP Connection Using Non-authenticated Proxy Server

Example

The following example provides the AT command sequence to open HTTP connection using Non-Authenticated Proxy server.

- **Enable the DHCP client on the GS node.**

```
AT+NDHCP=1
```

```
OK
```

- **Associate with a network**

```
AT+WA=GainSpan,,6
```

```
IP SubNet Gateway
```

```
192.168.23.45:255.255.255.0:192.168.23.1
```

```
OK
```

- **Configure the IP address of Proxy server.**

```
AT+HTTPCONF=11,192.168.2.117
```

- **Configure basic authentication of the final HTTP server.**

```
AT+HTTPCONF=2,Basic dGVzdDp0ZXN0MTIz
```

- **Configure IP address of the Proxy server with the port number.**

```
AT+HTTPOPEN=192.168.2.117,80
```

```
/**AT+HTTPOPEN=<HOST>,<PORT NUMBER>**/
```

```
0
```

```
OK
```

- **Send the final HTTP GET request from GS node to the final HTTP server along with the corresponding URI in the server.**

```
AT+HTTPSEND=0,1,100,http://192.168.2.223/test1kb.html
```

```
/**AT+HTTPSEND=<CID>,<TYPE>,<TIME OUT>,<PAGE>
```

```
Value of Type is 1 or 3,
```

```
1: HTTP GET
```

```
3: HTTP POST **/
```

3.13.16.2 Open HTTPS Connection Using Non-authenticated Proxy Server

Example

The following example provides the AT command sequence to open HTTPS connection using Non-authenticated proxy server by validating the CA certificate.

- Load CA certificate in the GS node.

```
AT+TCERTADD=ca,0,736,0
/**AT+TCERTADD=<NAME>,<FORMAT>,<SIZE>,<LOCATION>
NAME: Name of the certificate
FORMAT: 0, Binary (der format)
SIZE: Size of the certificate
LOCATION: Flash **/
OK
```

- Enable DHCP client on the GS node.

```
AT+NDHCP=1
OK
```

- Associate with a network.

```
AT+WA=GainSpan,,6
IP           SubNet          Gateway
192.168.23.45:255.255.255.0:192.168.23.1
OK
```

- Configure current system time of the GS node.

```
AT+SETTIME=16/12/2014,15:06:00
OK
```

- Display the current system time of the GS node.

```
AT+GETTIME=?
16/12/2014,15:6:5,1418742365360
OK
```

- Configure the Proxy server with the IP address and port number of the final HTTPS server.

```
AT+HTTPCONF=23,192.168.2.223:443
OK
```

- Configure IP address of the Proxy Server.

```
AT+HTTPCONF=11,192.168.2.117
OK
```

- Configure basic authentication of the final HTTPS server.

```
AT+HTTPCONF=2,Basic dGVzdDp0ZXN0MTIz
OK
```

- To open the HTTPS connection with final HTTPS server using Non-authenticated proxy server, configure the IP address of Proxy server with the port number.

```
AT+HTTPOPEN=192.168.2.117,80,1,,1
/**AT+HTTPOPEN=<HOST>,<PORT NUMBER>,<SSL FLAG>,,<PROXY>**/
0
OK
```

- Send the final HTTPS GET request from GS node to the final HTTPS server along with the corresponding URI in the server

```
AT+HTTPSEND=0,1,100,https://192.168.2.223/test1kb.html
/**AT+HTTPSEND=<CID>,<TYPE>,<TIME OUT>,<PAGE>
Value of TYPE is 1 or 3,
1: HTTPS GET
3: HTTPS POST**/
```

3.13.16.3 Open HTTPS Connection Using Domain Name Verification

GS module verifies the domain name given in the command against the domain name in the incoming server certificate when opening an HTTPS connection.

Example 1

The following example provides the AT command sequence to open HTTPS connection by verifying domain name when log level is set as 1.

- Enable DHCP client on the GS node.

```
AT+NDHCP=1
OK
```

- Associate with a network.

```
AT+WA=GainSpan,,6
IP SubNet Gateway
192.168.23.45:255.255.255.0:192.168.23.1
OK
```

- Configure current system time of the GS node.

```
AT+SETTIME=26/02/2015,15:06:00
OK
```

- Enable the Domain name check and specify the buffer size which is used to store alternative names provided in the incoming server certificate. The following command stores 100 bytes of alternate names (domain names) in the buffer.

```
AT+SSLCONF=1,100
/**AT+SSLCONF=<Domain name check>,<Buffer size>**/
OK
```

- Configure log level to 1 to view warning message when domain name verification fails.

```
AT+LOGLVL=1
//When AT=LOGLVL is configured as:
0: No warning is provided
1: Warning provided with name mismatch
2: Warning provided along with the alternate names (domain names)
provided in the incoming server certificate**/
OK
```

- Open the HTTPS connection with the host name. If there is a mismatch of host name GS module sends a warning message as shown below.

```
AT+HTTPOPEN=mtsindia.yahoo.com,,1
/**AT+HTTPOPEN=<Host>,,<SSLFlag>**/
IP:46.228.47.115
1
warning: certificate mismatch
```

OK

Example 2

The following example provides the AT command sequence to open HTTPS connection by verifying domain name when log level is set as 2.

- **Enable DHCP client on the GS node.**

AT+NDHCP=1

OK

- **Associate with a network.**

AT+WA=GainSpan,,6

IP SubNet Gateway

192.168.23.45:255.255.255.0:192.168.23.1

OK

- **Configure current system time of the GS node.**

AT+SETTIME=26/02/2015,15:06:00

OK

- **Enable the Domain name check and specify the buffer size which is used to store alternative names provided in the incoming server certificate. The following command stores 100 bytes of alternate names (domain names) in the buffer.**

AT+SSLCONF=1,100

/**AT+SSLCONF=<Domain name check>,<Buffer size>**/

OK

- **Configure log level to 2 to view warning message as well as the buffer content when domain name verification fails.**

AT+LOGLVL=2

/When AT=LOGLVL is configured as:

0: No warning is provided

1: Warning provided with name mismatch

2: Warning provided along with the alternate names (domain names) provided in the incoming server certificate**/

OK

- **Open the HTTPS connection with the host name. If there is a mismatch of host name GS module sends a warning message along with the buffer content since the log level is set to 2 as shown below.**

AT+HTTPOPEN=mtsindia.yahoo.com,,1

IP:46.228.47.115

1

warning: certificate mismatch:

www.yahoo.com

www.yahoo.com

yahoo.com

hsrd.yahoo.com

us.yahoo.com

fr.yahoo.com

uk.yahoo.com

OK

3.13.17 HTTP Client Data Exchange

This command is used to Get/Post HTTP data on the HTTP client. The content can be transferred using the escape sequence mentioned previously.

Command Syntax

```
AT+HTTPSEND=<CID>,<Type>,<Timeout>,<Page>[,Size of the  
content]<CR><LF>ESC<H><CID><Content of above size>
```

Parameter Description

Table 191, page 211 describes the HTTP Client Get/Post parameters.

Table 191 HTTP Client Get/Post Parameters

Parameter	Optional/Mandatory	Value	Description
CID	Mandatory	N/A	HTTP client identifier
Type	Mandatory	N/A	GSN_HTTP_METHOD_GET (1) GSN_HTTP_METHOD_HEAD (2) GSN_HTTP_METHOD_POST (3) GSN_HTTP_METHOD_PUT (4) GSN_HTTP_METHOD_DELETE (5) GSN_HTTP_METHOD_GETRESP (6) GSN_HTTP_METHOD_POSTRESP (7)
Page	Mandatory	N/A	The page/script being accessed (e.g., /index.html)
Timeout	Mandatory	N/A	Timeout value is in seconds
Size	Mandatory	N/A	Actual content size Optional in case of GET

In case the HTTP connection is opened with SSL encryption enabled, this command encrypt the data based with encrypt key in SSL connection structure for the specific CID. This encryption happens before Network Layer and the Encrypted data will be sent through the network layer

Receive is implicit in AT+HTTPSEND based on the HTTPS Server's response to the sent data. Received data is asynchronous and should be handled accordingly.

The response from the server is sent to the host in one or more chunks with maximum size of 2048 bytes. Each chunk is of the format:

```
<ESC>H<1Byte-CID><4 bytes-Length of the data><data>
```

The data part of first chunk of the response will have the status line at the beginning. The status line contains the status code and the status phrase. This will be in the format:

```
<status code><space><status phrase>\r\n
```

After the last chunk, OK/ERROR is sent to the host.

3.13.18 HTTP Client Close

This command is used to close the HTTP client connection identified by the CID.

Command Syntax AT+HTTPCLOSE=<CID>

3.13.19 Data Transfer in Bulk Mode

This command is used to enable or disable the bulk mode data transfer.

Command Syntax AT+BDATA=n

Parameter Description

Table 192, page 212 describes the Enable/Disable Bulk Mode Data Transfer parameters.

Table 192 Enable/Disable Bulk Mode Data Transfer Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	1	Enable Bulk Mode Data Transfer
		0 (default)	Disable Bulk Mode Data Transfer

3.13.20 Data Drop

This command is used to enable or disable dropping input data at Serial-to-WiFi level when socket failure or disconnect happens.

Command Syntax AT+DROPDATAEN=n

Parameter Description

Table 192, page 212 describes the Data drop parameters.

Table 193 Data Drop Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	1: Enable	Enable dropping input data at Serial-to-WiFi level when there is a socket failure or disconnection.
		0: Disable (default)	Disable dropping input data at Serial-to-WiFi level when there is a socket failure or disconnection.

When Data drop command is enabled, the behavior of <ESC> S and <ESC> Z are as follows:

When <ESC> S <CID> is executed,

- <ESC> S validates the specified CID.
- If the CID is invalid, then S2W remains in command mode until <ESC> E is received.
- If CID gets closed in between, then “ERROR” is displayed on the terminal and data is dropped.
- MCU needs to send <ESC> E sequence to execute AT command.

When <ESC> Z <CID> is executed for bulk data mode,

- <ESC> Z validates the specified CID>
- If the CID is invalid, then S2W remains in data mode, receives complete sequence, and displays “ERROR” on the terminal.

When Data drop command is disabled, the behavior of <ESC> S and <ESC> Z are as follows:

When <ESC> S <CID> is executed,

- <ESC> S validates the specified CID.
- If the CID is invalid, then S2W is moved to command mode.
- If CID gets closed in between, then “ERROR” is displayed on the terminal after each data transmission failure.
- MCU needs to send <ESC> E sequence to execute AT command.

When <ESC> Z <CID> is executed for bulk data mode,

- <ESC> Z validates the specified CID>
- If the CID is invalid at start of sequence (<ESC> Z), then S2W is moved to command mode.

3.14 Unassociated Frame Transmission and Reception

3.14.1 Unassociated Mode

This command is used to transmit and receive 802.11 management frames, control frames, or data frames without associating with an Access Point based on the configured parameters.

Command Syntax

```
AT+UNSOLICITEDTX=<Frame Control>,<Sequence Control>,
<Channel>,<Data Rate>,<Power>,<CCA Enable/Disable>,<Frame
Length>,<Reception Wait time>,<Address 1>,[<Address 3>],
[<Address 4>],[capture transmission timestamp in
ticks],[Reception frame type],[Enable/Disable IE filter
for reception frames],[Reception IE ID]
```

After issuing this command, the user needs to send the payload data as follows:

```
<ESC>D/d<PayLoad of the above Frame length>
```



NOTE: Size of Payload has to be in multiples of 4.

Parameter Description

Table 194, page 214 describes the Unassociated mode data transmission or reception parameters.

Table 194 Unassociated Mode Data Transmission or Reception Parameters

Parameter	Optional/Mandatory	Value	Description
Frame Control	Mandatory	Refer 802.11 specification.	It is the frame control field in the 802.11 frame. For more information, refer the 802.11 specification.
Sequence Control	Mandatory	0-65535	This field consists of two fields, 12 bits (LSB) of fragment number and 4 bits of (MSB) sequence number. For more information, refer 802.11 specification.
Channel	Mandatory	1-14	It is the channel used to send data.
Data Rate	Mandatory	Refer 802.11 specification.	It is the data rate used to transmit frames. For more information, refer 802.11 specification.
Power	Mandatory	Refer Table 195, page 217	It provides a range of power that is used to transmit data.

Table 194 Unassociated Mode Data Transmission or Reception Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
CCAEnable	Mandatory	1 or 0 • 0: Enable • 1: Disable	It is used to enable or disable clear channel assessment.
Frame Length	Mandatory	1400 Unit: bytes	It is the length of the payload. The maximum size of the frame is limited to 1400 bytes.
Reception wait time	Mandatory	0 - 4294967295 Unit: milliseconds • 0: The receiver does not wait for any frames. • 4294967295: The receiver is switched on until AT+UNSOLICITEDRXSTOP command is issued.	It is the duration in milliseconds to keep the receiver switched on after transmission to receive other frames of interest.
Address 1	Mandatory	Refer 802.11 specification	Refer 802.11 specification
Address 3	Optional	Refer 802.11 specification	Refer 802.11 specification
Address 4	Optional	Refer 802.11 specification	Refer 802.11 specification
Capture transmission time-stamp in ticks	Optional	0 or 1 • 0: Enable • 1: Disable	It is the captured time-stamp in ticks at the MAC layer after successful frame transmission. Each tick is 25 nano seconds as the reference clock is 40 MHz clock.

Table 194 Unassociated Mode Data Transmission or Reception Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
Reception frame type	Optional	<p>Types of frames with their values are as follows:</p> <ul style="list-style-type: none"> • 1: Beacon frame • 2: Probe request frame • 4: Probe response frame • 8: Multi cast data frame • 16: Unicast data frame • 32: Unicast frame from overlapping BSS • 64: Directed management frame (Note: All directed management frames except probe request, beacon, and probe response) • 256: Broadcast/multicast management frame • 512: Overlapping BSS unicast management frame • 1024: Broadcast/multicast management frame from overlapping BSS • 2048: Miscellaneous management frames • 4096: CTS frame • 8192: RTS frame • 16384: Non-directed control frames • 1073741824: Enable duplicate frame reception • 2147483648: Pass data to application with MAC headers 	It specifies the type of the frame to be received.
Enable/Disable IE filter for reception frames	Optional	<p>1, 0</p> <ul style="list-style-type: none"> • 1: Enable IE based filtering • 0: Disable IE based filtering 	<p>It is used to enable or disable a filter for reception frames based on the frame IDs configured in Reception IE ID parameter.</p>
Reception IE ID	Optional	Refer 802.11 specification.	<p>It is used to filter a frame based on the configured Information Element (IE) within a frame.</p> <p>Note:</p> <ul style="list-style-type: none"> • This parameter is valid only when Enable/Disable IE filter for reception frames is enabled. • Filtering is applicable for Beacons, Probe request and Probe response frames.

Table 195, page 217 provides the transmission rate and the corresponding input value range for Power in unassociated mode data transmission command.

Table 195 Transmission Rate and input value range for Power

Transmission Rate	Input Value Range for Power
1	1 to 8
2	1 to 4
5.5	1 to 7
6	1 to 13
6.5	1 to 13
9	1 to 13
11	1 to 5
12	1 to 13
18	1 to 13
19.5	1 to 13
24	1 to 13
26	1 to 13
36	1 to 12
39	1 to 12
48	1 to 12
54	1 to 9
58.5	1 to 10
65	1 to 8

Synchronous Response

Table 196, page 217 describes the synchronous responses and remarks for Unassociated mode data transmission command.

Table 196 Unassociated Mode Data Transmission Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	Failure If parameters are not valid.

Example 1

For sending Data frame where sequence number is 0 and fragment number is 0 in Sequence Control field:

The hex value for the Sequence Control field = 0x0000

The decimal value for the Sequence Control field = 0

```
AT+UNSOLICITEDTX=8,0,1,2,1,1,10,0,20:f8:5e:aa:25:05
```

Example 2 For sending Data frame where sequence number is 1 and fragment number is 0 in Sequence Control field:

The hex value for the Sequence Control field = 0x0010

The decimal value for the Sequence Control field = 16

```
AT+UNSOLICITEDTX=8,16,1,2,1,1,10,0,20:f8:5e:aa:25:05
```

Example 3 For sending Data frame where sequence number is 973 and fragment number is 0 in Sequence Control field:

The hex value for the Sequence Control field = 0x3cd0

The decimal value for the Sequence Control field = 15568

```
AT+UNSOLICITEDTX=8,15568,1,2,1,1,10,0,20:f8:5e:aa:25:05
```

Example 4 For sending Management (Beacon) frame,

```
AT+UNSOLICITEDTX=128,1,1,2,1,0,10,0,ff:ff:ff:ff:ff:ff
```

Example 5 For sending Control (RTS) frame,

```
AT+UNSOLICITEDTX=180,1,1,2,1,0,10,0,00:1d:c9:aa:bb:dd,00:  
1d:c9:aa:bb:ee
```

Example 6 For sending Control (CTS) frame,

```
AT+UNSOLICITEDTX=196,1,1,2,1,0,10,0,00:1d:c9:aa:bb:dd,00:  
1d:c9:aa:bb:ee
```

3.14.2 Start Data Reception in Unassociated Mode

This command is used to receive 802.11 management frames, control frames, or data frames on a specific channel without associating with an Access Point based on the configured parameters.

Command Syntax

```
AT+UNSOLICITEDRX=<Frame type>,<Enable/Disable IE filter  
for reception frames>,<Reception IE  
ID>,<Channel>,<Reception wait time>
```

Parameter Description

Table 197, page 220 describes the Unassociated Data Reception parameters.

Table 197 Unassociated Data Reception Parameters

Parameter	Optional/Mandatory	Value	Description
Frame type	Mandatory	<p>Types of frames:</p> <ul style="list-style-type: none"> • 1: Beacon frame • 2: Probe request frame • 4: Probe response frame • 8: Multi cast data frame • 16: Unicast data frame • 32: Unicast frame from overlapping BSS • 64: Directed management frame (Note: All directed management frames except probe request, beacon, and probe response) • 256: Broadcast/multicast management frame • 512: Overlapping BSS unicast management frame • 1024: Broadcast/multicast management frame from overlapping BSS • 2048: Miscellaneous management frames • 4096: CTS frame • 8192: RTS frame • 16384: Non-directed control frames • 1073741824: Enable duplicate frame reception • 2147483648: Pass data to application with MAC headers 	It specifies the type of frames to be received.
Enable/Disable IE filter for reception frames	Mandatory	<p>1 or 0</p> <ul style="list-style-type: none"> • 1: Enable IE based filtering • 0: Disable IE based filtering 	It is used to enable or disable IE filter for reception frames based on the frame IDs configured in Reception IE ID parameter.

Table 197 Unassociated Data Reception Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
Reception IE ID	Mandatory	Refer 802.11 specification.	<p>It is used to filter a frame based on the configured Information Element (IE) within a frame.</p> <p>Note:</p> <ul style="list-style-type: none"> • This parameter is valid only when Enable/Disable IE filter for reception frames is enabled. • Filtering is applicable for Beacons, Probe request and Probe response frames.
Channel	Mandatory	1-14	It is the channel used to send data.
Reception wait time	Mandatory	0 - 4294967295 Unit: milliseconds <ul style="list-style-type: none"> • 0: The receiver does not wait for any frames. • 4294967295: The receiver is switched on until AT+UNSOLICITEDRXSTOP command is issued. 	It is the duration in milliseconds to keep the receiver switched on to receive other frames of interest.

Command Response This command returns the standard command response.

Once the unsolicited frame is received by the adapter, it is sent to the serial interface in the following format.

```
<ESC>D<1 byte of RSSI in hex><2 bytes of length in hex><1 byte of frame type><3 bytes of reserved><4 bytes of time stamp in ticks><Data with MAC header/Data with Ethernet header>
```

- 1 byte of RSSI is a signed value in hexadecimal format.
- 2 bytes of length in hexadecimal format which specifies the length of data.
- 1 byte of frame type which is reserved for future. This parameter is in hexadecimal format which specifies the type of frame received. Types of frames to be supported are:
 - 0x01: Beacon
 - 0x02: Probe request
 - 0x03: Probe response
 - 0x04: Unicast data
 - 0x05: Multicast data
 - 0x06: CTS

- 0x07: RTS
- 0x08: Associated request
- 0x09: Associated response
- 0x0F: Raw data with MAC header
- 3 bytes of reserved field which is left empty.
- 4 bytes of time stamp in ticks which specifies the reception time-stamp of the frame at MAC layer. Each tick is 25 nano seconds as the reference clock is 40 MHz clock.
- Data of two types:
 - Data with MAC header: Data which is received as it is at the MAC layer without changing its format.
 - Data with Ethernet header: MAC header is removed from the received data and Ethernet header is added with fields: <6 bytes of Destination MAC>, <6 bytes of Source MAC>, <2 bytes of frame type>, <Real data>

Example

For receiving Management (Beacon) frame,

AT+UNSOLICITEDRX=2147483649,0,,1,1000

For receiving Data frame,

AT+UNSOLICITEDRX=16,0,,1,10000

For receiving Control (RTS/CTS) frame,

AT+UNSOLICITEDRX=28672,0,,1,10000

3.14.3 Stop Data Reception in Unassociated Mode

This command is used to stop the unsolicited data reception.

Command Syntax

AT+UNSOLICITEDRXSTOP

3.15 ISO TX

3.15.1 ISO TX Transmission Start

This command is used to start the ISO TX transmission.

Command Syntax

```
AT+ISOBLINK=<Mode>,<gain(power)>,<Number of sub-blanks>,
<Number of blinks>,<Blink interval>,<Message length><Tag
ID>,[<Bandwidth>,<Payload>,<Frequency>]
```

Parameter Description

Table 198, page 223 describes the ISO TX Transmission Start parameters.

Table 198 ISO TX Transmission Start Parameters

Parameter	Optional/Mandatory	Value	Description
Mode	Mandatory	<ul style="list-style-type: none"> • D: DSS • O: OOK/FSK • Q: QPSK 	It specifies the mode to be set.
gain(power)	Mandatory	Tx power: 1-15	It specifies the transmission power.
Number of sub-blanks	Mandatory	1-8	It specifies the number of sub-blanks.
Number of blinks	Mandatory	1-255	It specifies the number of blinks.
Blink interval	Mandatory	0 - 4294967295 Unit: milliseconds <ul style="list-style-type: none"> • 0: The receiver does not wait for any frames. • 4294967295: The receiver is switched on until AT+UNSOLICITEDRXSTOP command is issued. 	It specifies the blink interval.
Message length	Mandatory	DSS and QPSK: 56, 72, 152 OOK or FSK: 88, 184	It specifies the length of the message based on the mode.
Tag ID	Optional	32 bits	It specifies the tag ID.
Bandwidth	Mandatory	0: 30MHz 1: 19.5 MHz (Japan)	It specifies the bandwidth used.
Payload	Mandatory	16 bits	It specifies the payload.
Frequency	Mandatory	in Hertz	It specifies the frequency used.

Example

```
AT+ISOBLINK=D,15,4,25,1,56,33445566
AT+ISOBLINK=D,10,4,5,5,56,33445566
AT+ISOBLINK=D,10,4,5,5,56,33445566,1
AT+ISOBLINK=D,10,4,5,5,72,33445566,0,1234
AT+ISOBLINK=D,10,4,5,5,152,33445566
AT+ISOBLINK=D,10,4,5,5,56,33445566,0,0,2441750000
```

3.16 GSLINK

The adapter provides mechanism to send and receive raw HTTP Data as well as the data in XML format. The data can be sent and received either as a complete data as part of HTTP message as one (raw HTTP method) or it can be sent and received as XML data and each element can be sent and received individually.

This is the case when the GainSpan node is acting as HTTP Server and is sending or receiving data. In case of GainSpan node being HTTP Client it would know the type of communication it is doing with the server and can choose the raw HTTP or XML format of communication because the communication is initiated by the GainSpan node.

The raw HTTP communication means the complete XML data is sent or received by the Host as one data unit. In case of XML format, each element of the XML can be written individually and could be received individually helping the host parse and process easily.

3.16.1 Start/Stop Webserver

This command is used to start/stop the web server. This URI can be modified using the command specified in [3.16.5 URI Modification, page 234](#).

Command Syntax

AT+WEB SERVER=n,<user name>,<password>,[1=SSL enable/0=SSL disable],[idle timeout],[Response timeout]

Parameter Description

[Table 199, page 225](#) describes the Start/Stop Webserver parameters.

Table 199 Start/Stop Webserver Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0 (Stop)	If <i>n</i> is 1, start the webserver and n=0 stop the webserver.
		1 (Start)	
user name	Mandatory	admin (default)	If the user wants to use the default username from the SDK Builder, then issue DEFAULT. If username is not provided in the SDK Builder, “admin” will be used. If this parameter is left blank, then authentication is disabled.
password	Mandatory	admin (default)	If the user wants to use the default password from the factory default area, then issue DEFAULT. If the password is not provided in the factory default area, “admin” will be used.

Table 199 Start/Stop Webserver Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
SSL Enable/Disable	Optional	0 (Disable)	0 is for SSL disable, and 1 is for SSL enable.
		1 (Enable)	
Idle timeout (seconds)	Optional	120 seconds (default)	Idle time is the time at which GainSpan module waits for the HTTP data. If no data is transferred within the idle time then HTTP connection is removed by the client or node itself.
Response Timeout (milliseconds)	Optional	Maximum value - 100000 milliseconds (100 seconds)	Response timeout restricts the MCU to respond within a specified time.

Synchronous Response

Table 200, page 226 describes the synchronous responses and remarks for Start/Stop Webserver command.

Table 200 Start/Stop Webserver Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

Example

```
AT+WEB SERVER=1,admin,admin,0,5,10
OK
```

3.16.2 Enable or Disable XML Parser on HTTP Data

This command is used to enable or disable XML parser on HTTP data sent and received by the adapter.

Command Syntax

AT+XMLPARSE=n

Parameter Description

[Table 201, page 227](#) describes the Enabling/Disabling XML Parser on HTTP Data parameters.

Table 201 Enabling/Disabling XML Parser on HTTP Data Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0 (disable)	If <i>n</i> is 0, XML parser is disabled. If <i>n</i> is 1, XML parser is enabled.
		1 (enable)	

Synchronous Response

[Table 202, page 227](#) describes the synchronous responses and remarks for Enabling/Disabling XML Parser on HTTP Data command.

Table 202 Enabling/Disabling XML Parser on HTTP Data Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid. (n value is other than 0 or 1)

3.16.3 Send XML/Raw HTTP Data

This section provides commands used to send XML or Raw HTTP elements one by one using <ESC>G or <ESC>H sequence respectively.

Command Syntax for XML

AT+XMLSEND=<CID>,<Type>,<Timeout>,<Page URI>,<Root tag name>[,<N>]

MCU sends the XML data using the following ESC sequence:

<ESC>G<CID> [Reserved Len Value]<Len>,<Tag name>:<Value>

ESC G is sent N times, one for each tag.

“len value” is the length of the string including <tag name>:<value>

Usage

Usage of Reserved Len Values:

- 9900 - 9990: Future Use
- 9999: Future Use
- 9998: Start of Element with sub-elements
- 9997: End of Element with sub-elements
- 9996: Attribute
- 0000: End of Data



NOTE: MCU should send complete data as mentioned in AT+XMLSEND or AT+HTTPSEND commands.

Parameter Description

Table 203, page 228 describes the XML Data Send parameters.

Table 203 XML Data Send Parameters

Parameter	Optional/Mandatory	Value	Description
CID	Mandatory	CID is the CID allocated by the adapter (1 byte ASCII (0-F))	CID is the ID of the HTTP connection opened.
Type	Mandatory	6 (GETRESP) 7 (POSTRESP)	Type is either GETRESP or POSTRESP
Timeout	Mandatory	AT+XMLSEND=0,7, 100 ,/abc/environment/sensor,info,1,1,5get/post.	Timeout is the HTTP timeout for the get/post.

Table 203 XML Data Send Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
Page URI	Mandatory	/gainspan/profile/mcu(default) , AT+XMLSEND=0,7,100,/abc <i>/environment/sensor,info,1,1, 5</i>	Page URI is the URI of the page.
Root tag name	Mandatory	AT+XMLSEND=0.7,100,/abc <i>/environment/sensor,info,1,1, 5</i>	Root tag is the Root Tag of XML data.
N	Optional	AT+XMLSEND=0,7,100,/abc <i>/environment/sensor,info,1,1,5</i>	N is the number of elements in the XML string.

Synchronous Response

Table 204, page 229 describes the synchronous responses and remarks for XML Parser on HTTP Data Send command.

Table 204 XML Data Send Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

Example

```
AT+XMLSEND=0,7,100,/abc/environment/sensor,element1,1<ESC
><G>00009STATUS:OK
```

Parameter Description

Table 205, page 229 describes the XML data receive (ESC G) parameters.

Table 205 XML Data Receive (ESC G) Parameters

Parameter	Optional/Mandatory	Value	Description
ESC G	N/A	N/A	This is sent repeatedly for each tag for the XML data.
CID	N/A	1 byte	CID allocated by the adapter (1 byte ASCII (0-F)).
Length	N/A	4 bytes	Length is the length of the string including <tag name>:<value> in 4 bytes ASCII decimal value.
Type	N/A	3 or 1	Type is POST (3) or GET (1)
URI	N/A	N/A	URL is fetched by the Remote HTTP client.

Synchronous Response

Table 206, page 230 describes the synchronous responses and remarks for XML Data Receive (ESC G) command.

Table 206 XML Data Receive (ESC G) Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

Command Syntax for raw HTTP

AT+HTTPSEND=<CID>,<Type>,<Timeout>,<Page>,<Size of the content>

MCU sends raw HTTP data using the following Escape <ESC> sequence:

<ESC>H<CID><Length of the data><data>

Parameter Description

Table 203, page 228 describes the Raw HTTP Data Send parameters.

Table 207 Raw HTTP Data Send Parameters

Parameter	Optional/Mandatory	Value	Description
CID	Mandatory	N/A	HTTP client identifier
Type	Mandatory	N/A	GSN_HTTP_METHOD_GETRESP (6) GSN_HTTP_METHOD_POSTRESP (7)
Page	Mandatory	N/A	The page/script being accessed (e.g., /index.html)
Timeout	Mandatory	N/A	Timeout value is in seconds
Size	Mandatory	N/A	Actual size of the content

Synchronous Response

Table 204, page 229 describes the synchronous responses and remarks for Raw HTTP Data Send command.

Table 208 Raw HTTP Data Send Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

Parameter Description

Table 205, page 229 describes the raw HTTP data receive (ESC H) parameters.

Table 209 Raw HTTP Data Receive (ESC H) Parameters

Parameter	Optional/Mandatory	Value	Description
ESC H	N/A	N/A	This is sent repeatedly for each tag for the raw HTTP data.
CID	N/A	1 byte	CID allocated by the adapter (1 byte ASCII (0-F)).
Length of data	N/A	4 bytes	Length is the length of the string including <tag name>:<value> in 4 bytes ASCII decimal value.
data	N/A	3 or 1	Actual content

Synchronous Response

Table 206, page 230 describes the synchronous responses and remarks for raw HTTP Data Receive (ESC H) command.

Table 210 Raw HTTP Data Receive (ESC H) Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.16.4 Receive XML\Raw HTTP Data

When web client sends a request (XML or raw HTTP) to web server (GS Node), the GS node passes the request to MCU using the following Escape <ESC> sequence.

Command Syntax for XML GS node passes the request to MCU using the following Escape <ESC> sequence:

ESC K<CID><Reserved length value><Length><Type><URI>

Parameter Description

Table 211, page 232 describes the XML data receive (ESC K) parameters.

Table 211 XML Data Receive (ESC K) Parameters

Parameter	Optional/Mandatory	Value	Description
ESC K	Mandatory	N/A	This is sent once the URL is fetched by the Remote HTTP client.
CID	Mandatory	1 byte	CID allocated by the adapter (1 byte ASCII (0-F)).
Reserved length value	Mandatory	N/A	This specifies the type of data sent to MCU. <ul style="list-style-type: none">• 9998: Start of Element with sub elements• 9997: End of Element with sub elements• 9996: Attribute• 0000: End of Data
Length	Mandatory	4 bytes	Length is the length of the string including <tag name>:<value> in 4 bytes ASCII decimal value.
Type	Mandatory	1 or 3	Type is GET (1) or POST (3)
URI	Mandatory	N/A	URL is fetched by the Remote HTTP client.

Synchronous Response

Table 212, page 233 describes the synchronous responses and remarks for XML Data Receive (ESC K) command.

Table 212 XML Data Receive (ESC K) Synchronous Responses

Responses	Remarks
OK 0	Success
ERROR:INVALID INPUT 2	If parameters are not valid.

3.16.5 URI Modification

This command is used to modify the default adapter URI.

Command Syntax AT+URIRECV=<URI> [, Content Type]

Usage Usage of Reserved Length Values

- 9000 to 9999 - Reserved for future use

Parameter Description

Table 213, page 234 describes the URI Modification parameters.

Table 213 URI Modification Parameters

Parameter	Optional/ Mandatory	Value	Type	Description
URI (Uniform Resource Identifier)	Mandatory	/gainspan/profile/mcu (default), /gainspan/system (reserved) Maximum length of URI is 64 characters including the null terminating character ('0').	N/A	URI is a string used to identify a web resource.
Content Type	Optional	0	application/xml (default)	Content type for the URI.
		1	application/json	
		2	application/html	
		3	Img/gif	
		4	application/octet-stream	

Synchronous Response

Table 215, page 234 describes the synchronous responses and remarks for URI Modification command.

Table 215 URI Modification Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.17 CoAP

3.17.1 CoAP Client Option Configuration

This command upon reception the adapter configures the CoAP parameters.

Command Syntax AT+COAPOPTCONF=<Parm>, <Value>

Parameter Description

Table 216, page 235 describes the CoAP Client Option Configuration parameters.

Table 216 CoAP Client Option Configuration Parameters

Parameter	Values
GSN_COAP_OPTION_IF_MATCH (1)	N/A
GSN_COAP_OPTION_URI_HOST (3)	
GSN_COAP_OPTION_ETAG (4)	
GSN_COAP_OPTION_IF_NONE_MATCH (5)	
GSN_COAP_OPTION_URI_PORT (7)	
GSN_COAP_OPTION_URI_PATH (11)	
GSN_COAP_OPTION_CONTENT_FORMAT (12)	<ul style="list-style-type: none"> • text/plain; charset=utf-8 (0) • application/line-format (40) • application/xml (41)¹ • application/octet-stream (42) • application/exi (47) • application/json (50)
GSN_COAP_OPTION_MAX_AGE (14)	N/A
GSN_COAP_OPTION_URI_QUERY (15)	
GSN_COAP_OPTION_ACCEPT (16) ³	<ul style="list-style-type: none"> • text/pain; charset=utf-8 (0) • application/line-format (40) • application/xml (41)¹ • application/octet-stream (42) • application/exi (47) • application/json (50)
GSN_COAP_OPTION_TOKEN (19) ²	<ul style="list-style-type: none"> • Auto Generate (0) • Any Value (1 to 8 bytes)
GSN_COAP_OPTION_PROXY_URI (35)	N/A



NOTE: The value is a string that depends on the parameters in the above table.

- Note: 1. When using CoAP with XML the only valid value is 41.
Note: 2. If the Token Option is not set, no Token Option is sent.
Note: 3. To specify more than one Accept Option, the values must be given with a “.” separator with the priority from left to right.

Synchronous Response

Table 217, page 236 describes the synchronous responses and remarks for CoAP Client Option Configuration command.

Table 217 CoAP Client Option Configuration Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure

3.17.2 CoAP Client Option Configuration Removal

This command upon reception the adapter removes the CoAP configuration specified by the “param”.

Command Syntax AT+CoAPOPTCONFDEL=<Param>

Parameter Description

Table 218, page 236 describes the CoAP Client Option Configuration Removal parameters.

Table 218 CoAP Client Option Configuration Removal Parameters

Parameter
GSN_COAP_OPTION_IF_MATCH (1)
GSN_COAP_OPTION_URI_HOST (3)
GSN_COAP_OPTION_ETAG (4)
GSN_COAP_OPTION_IF_NONE_MATCH (5)
GSN_COAP_OPTION_URI_PORT (7)
GSN_COAP_OPTION_URI_PATH (11)
GSN_COAP_OPTION_CONTENT_FORMAT (12)
GSN_COAP_OPTION_MAX_AGE (14)
GSN_COAP_OPTION_URI_QUERY (15)
GSN_COAP_OPTION_ACCEPT (16)
GSN_COAP_OPTION_TOKEN (19)
GSN_COAP_OPTION_PROXY_URI (35)

Synchronous Response

[Table 219, page 237](#) describes the synchronous responses and remarks for CoAP Client Option Configuration Removal command.

Table 219 CoAP Client Option Configuration Removal Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure

3.17.3 CoAP Client Connection Open

This command is used to create CoAP content and return CID.

This command is used to open a CoAP client on the adapter and connects to the server specified by the host name or IP address in case of DTLS flag is set to 1. If the DTLS flag is set to 1, then the other parameters like host, port number, etc. needs to be provided. If DTLS flag is set to 0, a CoAP content is created and CID is returned.

Command Syntax AT+CoAOPEN=<DTLS Flag>

Parameter Description

[Table 220, page 237](#) describes the CoAP Client Connection Open parameters.

Table 220 CoAP Client Connection Open Parameters

Parameter	Optional/Mandatory	Value	Description
DTLS Flag	Mandatory	0, 1 • 0 - CoAP content is created and CID is returned • 1 -	DTLS Flag is set to 0 as DTLS is not supported in this version.

Note:

Synchronous Response

[Table 221, page 237](#) describes the synchronous responses and remarks for CoAP Client Connection Open command. It returns the normal response code and the CID of the CoAP client connection on success.

Table 221 CoAP Client Connection Open Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure

3.17.4 CoAP Client Connection Send

This command is used to send a CoAP client on the adapter and connect to the server specified by the host name or IP address.

Command Syntax

```
AT+CoAPSENDRECEIVE=<CID>,<coap-uri>,<connection
method>,<connection type>,<response
Timeout>,[<payloadsize>,<payload Type>,<payload>]
```

Parameter Description

Table 222, page 239 describes the CoAP Client Connection Send parameters.

Table 222 CoAP Client Connection Send Parameters

Parameter	Optional/Mandatory	Value	Description
CID	Mandatory		
coap-uri	Mandatory	N/A	CoAP URI is the fully qualified URI with host, port, path, etc. (e.g., coap://192.168.240.1:5683/gainspan/profile).
connection method	Mandatory	GET/POST	CoAP connection method.
connection type	Mandatory	CON/NON	CoAP connection type.
response timeout	Mandatory	Maximum value is 60 seconds	The time to wait before a response is received (in seconds). This is required to be set only if connection type is of type Non-Confirmable.
payload type	Optional	N/A	Content-type of the payload. Optional in case of GET.
payload size	Optional	N/A	Length of the payload sent with the request. Optional in case of GET.
payload	Optional	N/A	Payload to send with CoAP request. It is specified using ESC<P><CID><Content of the abovesize>. Optional in case of GET.

Command Note

In case of CoAP connection is opened with DTLS encryption enabled, this command encrypts the data based with encrypt key in DTLS connection structure for the specific CID. This encryption happens before Network Layer and the Encrypted data will be sent through the network layer.

Command Response

Receive is implicit in AT+CoAPSEND based on the CoAP Server's response to the sent data. Received data is synchronized and will be printed on the console.

Synchronous Response

Table 223, page 240 describes the synchronous responses and remarks for CoAP Client Connection Send command. It returns the normal response code and the CID of the CoAP client connection on success.

Table 223 CoAP Client Connection Send Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure

3.17.5 CoAP Client Connection Close

This command is used to close a CoAP client connection identified by the CID and returns the standard command response.

Command Syntax

AT+CoAPCLOSE=<CID>

3.18 Using CoAP with GSLink

When using CoAP with GSLink, the host must do the following:

- Configure the CoAP Option Parameters
- Configure the General CoAP Parameter
- Open CoAP Client Connection
- Use the CID returned by the CoAP Client as part of XML Send

3.19 Battery Check

3.19.1 Battery Check Start

This command is used to send out a unit of battery check frequency in number of packets from the Serial-to-WiFi adapter, and store the resulting values in nonvolatile memory. Only the most recent value is stored. Battery checks are performed during packet transmission to ensure that they reflect loaded conditions. Battery checks can be used to ensure that a battery-powered system is provided with sufficient voltage for normal operation. Low supply voltages can result in data corruption when profile data is written to flash memory.

Command Syntax AT+BCHKSTRT=<Frequency>

Parameter Description

Table 224, page 242 describes the Battery Check Start parameters.

Table 224 Battery Check Start Parameters

Parameter	Optional/Mandatory	Value	Description
Frequency	Mandatory	1-100 packets	<p>It specifies the number of packets GS node sends before performing the battery check.</p> <p>Example: When <i>Frequency</i> is configured as 10, GS node performs the battery check after every 10 packets are transmitted.</p>

Synchronous Response

Table 225, page 242 describes the synchronous responses and remarks for Battery Check Start command.

Table 225 Battery Check Start Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.19.2 Battery Warning/Standy Level Set

This command is used to set the battery warning/standby level to and enable the adapter's internal battery level monitoring logic starts. This command should be executed before the battery check start command (see [3.19.1 Battery Check Start, page 242](#)).

Command Syntax

`AT+BATTLVLSET=<Warning Level>,<Warning Frequency>,<Standby Level>`

Parameter Description

[Table 226, page 243](#) describes the Battery Warning/Standy Level Set parameters.

Table 226 Battery Warning/Standy Level Set Parameters

Parameter	Optional/Mandatory	Value	Description
Warning Level	Mandatory	N/A	The battery voltage, in millivolts. When the adapter batter voltage is less than this level, it sends a message "Battery Low" to the serial interface.
Warning Frequency	Mandatory	N/A	This is the frequency at which the adapter sends the "Battery Low" message to the serial interface once the adapters battery check detected low battery.
Standby Level	Mandatory	N/A	The battery voltage, in millivolts. When the adapter battery voltage reaches this level, it sends the message "Battery Dead" to the serial interface and goes into a long Standby mode.

Synchronous Response

[Table 227, page 243](#) describes the synchronous responses and remarks for Battery Warning/Standy Level Set command.

Table 227 Battery Warning/Standy Level Set Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.19.3 Battery Check Set

This command is used to set/reset the battery check period after the battery check has been started. Upon receipt, the adapter records the new value of the battery check frequency so that adapter performs the battery voltage check with the new value set.

Command Syntax AT+BCHK=<Battery check frequency>

Alternate Command

The same command can be used to get the current configured battery check period, the usage as follows:

AT+BCHK=?

Parameter Description

Table 228, page 244 describes the Battery Check Set parameters.

Table 228 Battery Check Set Parameters

Parameter	Optional/Mandatory	Value	Description
Battery check frequency	Mandatory	1-100	The valid range for Battery check frequency is between 1 and 100.

Synchronous Response

Table 229, page 244 describes the synchronous responses and remarks for Battery Check Set command.

Table 229 Battery Check Set Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.19.4 Battery Check Stop

This command is used to halt battery check.

Command Syntax AT+BCHKSTOP

Command Response This command returns standard command response or ERROR, if the operation fails.

3.19.5 Battery Value Get

This command is used to retrieve the results of battery check operations.

Command Syntax AT+BATTVALGET

Command Response This command should return a message with the latest value, e.g., Battery Value: 3.4 V, followed by the standard command response.

If this command is issued before issuing the command to start battery checks, it returns ERROR or 1, depending on the current verbose setting.

3.20 Power State Management

3.20.1 Enable Deep Sleep

This command is used to enable the GainSpan SoCs power-saving Deep Sleep processor mode.

Command Syntax

AT+PSDPSLEEP

Usage

When enabled, the SoC will enter the power-saving Deep Sleep mode when no actions are pending. In Deep Sleep mode, the processor clock is turned off, and SoC power consumption is reduced.



NOTE: *Other components external to the SoC may continue to dissipate power during this time, unless measures are taken to ensure that they are also off or disabled.*

The processor can be awakened by sending data on the serial port from the host. However, several milliseconds are required to stabilize the clock oscillator when the system awakens from Deep Sleep. Since the clock oscillator must stabilize before data can be read, the initial data will not be received; “dummy” (discardable) characters or commands should be sent until an indication is received from the application.

Command Response

These commands do not return any response code to the serial interface. The S2W adapter sends the message “Out of Deep Sleep” along with the standard response once it comes out from deep sleep.

Parameter Description

A similar command can be used to enable the deep sleep with a timeout and alarm. [Table 230, page 247](#) describes the Enable/Disable SoC Deep Sleep parameters.

AT+PSDPSLEEP=<timeout>,<ALARM1 POL>[,<ALARM2 POL>]

Table 230 Enable/Disable SoC Deep Sleep Parameters

Parameter	Optional/Mandatory	Value	Description
ALARM1 POL	Mandatory	0 (high-to-low)	This is the polarity of the transition at pin RTC_IO_1 of the SoC will trigger an alarm input and waken the GainSpan SoC from deep sleep. A value of 0 specifies a high-to-low transition as active; a value of 1 specifies low-to-high.
		1 (low-to-high)	
ALARM2 POL	Optional	32-bit	This is the polarity of the transition at pin RTC_IO_2 that triggers an alarm input, using the same convention used for Alarm1. Upon reception of this command the adapter goes to the deep sleep state for timeout milliseconds and comes out. The maximum value of the timeout parameter can be the highest integer possible by 32 bit value.

Synchronous Response

Table 231, page 247 describes the synchronous responses and remarks for Enable/Disable SoC Deep Sleep command.

Table 231 Enable/Disable SoC Deep Sleep Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.20.2 Configure Power Save in Limited AP Mode

This command is used to configure power save in Limited AP mode.

Command Syntax

```
AT+WAPPSCFG=<Power-Save Configuration>,<Reserved parameter>,<Receiver on-time after Tx><Power-Save Behavioral Control>
```

Usage

When enabled, the SoC will enter the power saving mode when no actions are pending. In power save mode, the processor clock is turned off, and SoC power consumption is reduced.

Parameter Description

Table 232, page 248 describes power save in Limited AP Mode parameters.

Table 232 Deep Sleep in Limited AP Mode Parameters

Parameter	Optional/Mandatory	Value	Description
Power-Save Configuration	Mandatory	0,1	This parameter decides the state of radio (on/off) in conjunction with 'Power-Save Control' parameter.
Reserved parameter	Mandatory	0	Always issue zero (0) for this parameter.
Receiver on-time after Transmission	Mandatory	1	<p>It specifies the time the receiver will be kept on after any transmission (beacon). Unit: millisecond</p> <p>Example: When this parameter is configured as 10, the receiver will be switched on for 10 milliseconds after transmitting the beacons.</p> <p>Note:</p> <ul style="list-style-type: none"> a> If system decides to transmit a frame in the mean time (within 10ms as mentioned in the above example), then receiver on-time will restart from that instant. b> Maximum 'Receiver on-time after Transmission' should not exceed beacon interval.
Power-Save Control	Mandatory	0,1	This parameter decides the state of radio (on/off) in conjunction with 'Power-Save Configuration'. Refer to the Table 233, page 249 .

The following table provides behaviors of an AP corresponding to the combination of values configured for Power-Save Control and Power-Save Configuration parameters.

Table 233 AP behavior based on Power-Save Control and Power-Save Configuration

Power-Save Control	Power-Save Configuration	
	0	1
0	Exit power save immediately. (Radio will be switched on immediately) Note: Exits power save only after all pending transmit and receive events.	Enter power save immediately. (Radio will be switched off immediately) Note: Enters power save only after all pending transmit and receive events.
1	Exit power save at the next TBTT (beacon interval).	Enter power save only after all associated clients are in power save. Note: System will exit power save as soon as any one of the STA's exit the power save mode, but will not automatically re-enter the power save state. This is supported only from 5.2.x.

Synchronous Response

Table 234, page 249 describes the synchronous responses and remarks for Deep Sleep in Limited AM mode command.

Table 234 Deep Sleep in Limited AP Mode Synchronous Responses

Responses	Remarks
OK	Success
ERROR	Failure
ERROR:INVALID INPUT	If parameters are not valid.

3.20.3 Request Standby Mode

This command is used to request a transition to ultra-low-power Standby operation.

Command Syntax

AT+PSSTBY=x[, <DELAY TIME>, <ALARM1 POL>, <ALARM2 POL>]

Usage

When this command is issued, the GainSpan SoC will enter the ultra-low-power Standby state (after the optional delay time if present), remaining there until x milliseconds have passed since the command was issued, or an enabled alarm input is received. Any current CIDs are lost on transition to Standby. On wakeup, the adapter sends the message Out of Standby-<reason of wakeup> or the corresponding error code, depending on verbose status.

In Standby, only the low-power clock and some associated circuits are active. Serial messages sent to the UART port will not be received. The radio is off and packets cannot be sent or received. Therefore, before requesting a transition to Standby, the requesting application should ensure that no actions are needed from the interface until the requested time has passed, or provide an alarm input to awaken the SoC when needed. The alarm should trigger about 10 msec prior to issuance of any serial commands.

The dc_dc_cntl programmable counter is 48-bits and provides up to 272 years worth of standby duration. Standby is not entered until all pending tasks are completed, and a few milliseconds are required to store any changes and enter the Standby state; a similar delay is encountered in awaking from Standby at the end of the requested time. Therefore, we do not recommend Standby times less than about 32 milliseconds.



NOTE: Before the system enters Standby mode, the GainSpan SoC sends a NULL frame with PM bit set to 1. Once the system is out of Standby mode, the GainSpan SoC sends another NULL frame with PM bit set to 0. This behavior occurs only when radio is in Active ON mode.

Parameter Description

Table 235, page 250 describes the Request Standby Mode parameters.

Table 235 Request Standby Mode Parameters

Parameter	Optional/Mandatory	Value	Description
x	Mandatory	x =Standby time in milliseconds	This is the Standby time in milliseconds. If a delay time is provided, the Standby count begins after the delay time has expired.
DELAY TIME	Optional	in milliseconds	This is the delay in milliseconds from the time the command is issued to the time when the SoC goes to Standby.

Table 235 Request Standby Mode Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
ALARM1 POL	Optional	0 (high-to-low)	This is the polarity of the transition at pin RTC_IO_1 of the SoC which will trigger an alarm input and waken the GainSpan SoC from Standby. A value of 0 specifies a high-to-low transition as active; a value of 1 specifies low-to-high.
		1 (low-to-high)	
ALARM2 POL	Optional	N/A	This is the polarity of the transition at pin RTC_IO_2 that triggers an alarm input, using the same convention used for Alarm1.

Note: Specifying an alarm polarity also enables the corresponding alarm input.

Synchronous Response

Table 236, page 251 describes the synchronous responses and remarks for Request Standby Mode command.

Table 236 Request Standby Mode Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.21 Auto Connection

3.21.1 Wireless Parameters

This command is used to set the auto connection wireless parameters for the current profile. All other parameters required to configure the wireless connection are taken from the current Profile.

Command Syntax AT+WAUTO=<mode>, <SSID>, [<BSSID>], [channel]

Parameter Description

Table 237, page 252 describes the Wireless parameters.

Table 237 Wireless Parameters

Parameter	Optional/Mandatory	Value	Type	Description
mode	Mandatory	0 2	Infrastructure Limited AP	GainSpan module can be configured as an infrastructure mode or Limited AP mode.
SSID (Service Set Identifier)	Mandatory	Any valid SSID (see 2.6.3 SSID and Passphrase, page 51 for SSID format)	N/A	SSID is the SSID of the AP or Limited AP to connect to.
BSSID (Basic Service Set Identifier)	Optional	Any valid BSSID (17 character of the form xx:xx:xx:xx:xx:xx)	N/A	BSSID is the BSSID of the AP to connect to.
channel	Optional	1-14	N/A	N/A

Synchronous Response

Table 238, page 252 describes the synchronous responses and remarks for Wireless Parameters command.

Table 238 Wireless Parameters Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.21.2 Network Parameters

This command is used to set the network parameters for auto connection operation for the current profile. In Limited AP mode use UDP/TCP server type if using auto connection.

Command Syntax AT+NAUTO=<Type>,<Protocol>,<Destination IP/Host name>,<Destination Port>,[Src Port]

Parameter Description

Table 239, page 253 describes the Network parameters.

Table 239 Network Parameters

Parameter	Optional/Mandatory	Value	Description
Type	Mandatory	0, 1	Type is 0 for Client and 1 for Server. In Limited AP mode use UDP/TCP server type if using auto connection.
Protocol	Mandatory	0, 1	Protocol is 0 for UDP and 1 for TCP.
Destination IP/Host name	Mandatory	192.168.17.2	Destination IP is the IP address of the remote system (optional if the Adapter is acting as a server). Host Name is Domain name of the remote system. The adapter accepts either the destination IP or host name. The maximum length of the host name can be 32 ASCII characters.
Destination Port	Mandatory	16-bit unsigned integer, ranging from 1 to 65535 (port number 0 is reserved and can't be used).	Destination Port is the port number to connect to on the remote system.
Src Port	Optional	16-bit unsigned integer, ranging from 1 to 65535 (port number 0 is reserved and can't be used).	Src Port is the source port to bind and is valid only for UDP client case. This parameter is an optional one for UDP client and not valid for other protocol types.

Synchronous Response

Table 240, page 253 describes the synchronous responses and remarks for Network Parameters command.

Table 240 Network Parameters Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

Asynchronous Response

Table 241, page 254 describes the asynchronous responses and remarks for Network Parameters command.

Table 241 Network Parameters Asynchronous Responses

Responses	Remarks
N/A	In case of AT+WAUTO Asynchronous messages are expected only in layer 4 level. When GS node is TCP/UDP server, then CONNECT and DISCONNECT are asynchronous responses. When GS node is TCP/UDP client, then only DISCONNECT will be the asynchronous message.
N/A	TCP/IP connection successful. <CID> = the new CID in hexadecimal format. TCP/IP connection with the given CID is closed. This response is sent to the host when a connection is closed by the remote device.

Example



NOTE: Connection or disconnection commands such as AT+WA and AT+WD which are not used as Auto connection uses NCM in the background.

AT+ASYNCFMSGFMT=1

OK

AT+WAUTO=0, GainSpanDemo

OK

AT+NDHCP=1

OK

AT+NAAUTO=1, 1,, 3000

OK

AT&W0

OK

ATC1

OK

ATA

IP SubNet Gateway
192.168.17.2:255.255.255.0:192.168.17.1
OK

3.21.3 Enable Auto Connection

This command is used to store configuration settings in non-volatile memory and modify according to the parameter value in the command; the resulting change (if any) takes effect on the next reboot, or the next issuance of an ATA command.

Command Syntax ATCn

Parameter Description

Table 242, page 255 describes the Enable Auto Connection parameters.

Table 242 Enable Auto Connection Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0, 1 0: Disable 1: Enable	n is 0 to disable auto connection or 1 to enable auto connection.

Synchronous Response

Table 243, page 255 describes the synchronous responses and remarks for Enable Auto Connection command.

Table 243 Enable Auto Connection Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.21.4 Initiate Auto Connect

This command is used to start auto connection including association.

Upon reception of this command, the interface initiates the auto connection procedure as described in [2.2.1 Auto Connection, page 36](#), using the parameters specified by the AT+WAUTO and AT+NAUTO commands (see [3.21.1 Wireless Parameters, page 252](#) and [3.21.2 Network Parameters, page 253](#)).

Command Syntax

ATA

Usage

The adapter initiates auto connection but does not respond with any success or failure information. To check whether the auto connection is initiated, check GPIO19GPIO9 is high or low.

After the connection is established, the adapter enters the data transfer mode described in [2.2.1 Auto Connection, page 36](#).

Command Note

The GPIO8 should be kept low for the auto connection, since a low to high transition of this GPIO exits the auto connection data mode. After exiting from auto connect data mode using +++ or GPIO8 high, it is recommended to use ATO go back to auto connect data mode.

Example



NOTE: Connection or disconnection commands such as AT+WA and AT+WD are not used as Auto connection uses NCM in the background.

```
AT+WAUTO=0, GainSpanDemo
OK
```

```
AT+NDHCP=1
OK
```

```
AT&W0
OK
```

```
ATC1
OK
```

```
ATA
IP           SubNet          Gateway
192.168.17.2:255.255.255.0:192.168.17.1
OK
```

```
CONNECT 0 1 192.168.17.3 49756
```

3.21.5 Exit from Auto Connect Data Mode

In auto connect mode the adapter opens a serial data pipe to pass the serial data from/to the host MCU to/from the remote machine. In this mode, all serial inputs are treated as data. To enable the command mode without breaks, the connection the adapter provides uses the following mechanisms:

1. +++ and wait for 1 second. After this, the adapter exits from the data mode and supports to accept AT commands to change the configuration. +++ and wait for auto connection exit timeout (ATS8). This can be disabled by setting ATS8 as 0 so that +++ will be considered as data (See [3.7 Serial-to-WiFi Configuration, page 84](#)).
2. Make the GPIO8 high. After this, the adapter exits from the data mode and supports to accept AT commands to change the configuration.

3.21.6 Return to Auto Connect Mode

The command is used to return to auto connect mode.

Command Syntax ATO

Usage If the interface receives this command after it has exited the auto connect mode with +++ or GPIO8 high, it shall return to auto connect mode. If the connection no longer exists, the interface attempts to reestablish the previous connection, and returns to data mode if the reconnection is successful. If the Adapter was not previously connected when this command is received, it returns an error.

Command Response This command returns standard command response or ERROR, if the operation fails.



NOTE: Connection or disconnection commands such as AT+WA and AT+WD are not used as Auto connection uses NCM in the background.

3.21.7 Use Cases for Auto Connect Mode

This section provides examples for enhanced auto connection in Limited AP and station modes.

Example for Limited AP Mode AT+WM=2
OK

AT+APCONF=1
OK

AT+NSET=192.168.21.1,255.255.255.0,192.168.21.1
OK

AT+DHCPSRVR=1
OK

```
AT+WAUTO=2, GainSpanAP,, 6
OK
```

```
AT+N AUTO=1, 1,, 4001
OK
```

```
ATC1
OK
```

```
AT&W0
OK
```

```
ATA/AT+REST/Power cycle the node
OK
```

**Example for Station
Mode**

```
AT+NDHCP=1
OK
```

```
AT+WAUTO=0, GainSpanDemo
OK
```

```
AT+N AUTO=0, 1, 192.168.25.2, 9999
OK
```

```
ATC1
OK
```

```
AT&W0
OK
```

```
ATA/AT+REST/Power cycle the node
OK
```

3.22 Network Connection Manager (NCM)

The adapter supports network connection manager which manage L2, L3, and L4 level connection automatically. The parameters for L2, L3 and L4 can be configured using commands specified in [3.21.1 Wireless Parameters, page 252](#) and [3.21.2 Network Parameters, page 253](#). The security parameters can be configured using the commands specified in [3.11 WiFi Security Configuration, page 115](#).

3.22.1 NCM Start/Stop

This command is used to start/stop the network connection manager.

Command Syntax

```
AT+NCMAUTO=<Mode>, <Start/Stop>[, Level], [<Nvds store flag>]
```

Usage

If the NCM Start/Stop is stored in persistent storage, then the adapter will take the appropriate action for successive boots.

This command starts the NCM by connecting to the AP (if the mode configured as station) or create a limited AP (if the mode configured as limited AP) with the pre-configured parameters. Once it connected any of the L2, L3, and L4 disconnection triggers the NCM and it starts do the L2, L3, and L4 re-connection.

Once the connection is established the adapter returns the following message to the serial interface.

```
For L2+L3:  
IP address  
"NWCONN-SUCCESS"  
For L2+L3+L4:  
IP address  
"NWCONN-SUCCESS"  
"CONNECT <cid>"
```

For limited AP, the first two parameters are only valid and it outputs the same message for L2+L3 to the serial interface.



NOTE: If the DHCP renewal success with a new IP address then the adapter closes the sockets that are open (L4) and sends a message "IP CONFIG-NEW IP" with the new IP information to the serial interface and it retains the L4 connection if the NCM is started with L4 support.

Parameter Description

Table 244, page 260 describes the NCM Start/Stop parameters.

Table 244 NCM Start/Stop Parameters

Parameter	Optional/Mandatory	Value	Description
Mode	Mandatory	0	For station mode
		1	For limited AP mode
Start/Stop	Mandatory	0	For stop the NCM
		1	For start the NCM
Level	Mandatory	0	For L2+L3 connection
		1	For L2+L3+L4 connection
NVDS Store Flag	Mandatory	0 (default)	For storing the NCM Start/Stop information in the persistent storage when the store persistent information command (AT&W0) is issued by the host.
		1	For disabling the storage of this information. The default value is 0. This parameter is valid for NCM in station mode only.

Synchronous Response

Table 245, page 260 describes the synchronous responses and remarks for NCM Start/Stop command.

Table 245 NCM Start/Stop Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.22.2 NCM Configuration

This command is used to configure the NCM parameters for its state machine. This is the ID corresponding to the NCM configuration parameters. The L4 configuration parameters (L4 retry count and period) can be configured using ATS6/7 command.

Command Syntax

AT+NCMAUTOCONF=<Conf Id>,<Value>

Parameter Description

Table 246, page 261 describes the NCM Configuration parameters.

Table 246 NCM Configuration Parameters

Parameter	Optional/Mandatory	Conf Id	Value	Description
Conf Id, Value	Mandatory	0	1 to 65535 (default is 1000 milliseconds)	CPU Wait Period (1 to 6)
	Not Supported	1	1 to 65535 (default 1000 milliseconds)	Power Save Periods (not supported)
	Mandatory	2	1 to 65535 (default 1000 milliseconds)	Know Channel Scan Period
	Not Supported	3	1 to 65535 (default 1000 milliseconds)	Specific Channels Scan Period (not supported)
	Mandatory	4	1 to 65535 (default 1000 milliseconds)	All Channel Scan period
		5	1 to 65535 (default 1000 milliseconds)	Layer 3 Connect Period This specifies the Serial to WiFi level delay between each connection request. When a connection does not go through for a connection request, the network stack retries as per the configuration.
	Mandatory	6	Can be configured using the command ATS 6/7 in 3.7 Serial-to-WiFi Configuration, page 84	NCM Layer 4 Retry Period This specifies the Serial to WiFi level delay between each connection request. When a connection does not go through for a connection request, the network stack retries as per the configuration.
		7		NCM Layer 4 Retry Count This specifies the Serial to WiFi level retry count. When a connection does not go through for a connection request, the network stack retries as per the configuration.

Table 246 NCM Configuration Parameters (Continued)

Parameter	Optional/Mandatory	Conf Id	Value	Description
Conf Id, Value	Mandatory	8	1 to 65535 (default 10)	Known channel scan retry count
Conf Id, Value	Not Supported	9	1 to 65535 (default 10)	Specific channels scan retry count (not supported)
Conf Id, Value	Mandatory	10	1 to 65535 (default 10)	All Channel scan retry count
Conf Id, Value	Mandatory	11	1 to 65535 (default 100)	Layer 3 Connect retry count This specifies the Serial to WiFi level retry count. When a connection does not go through for a connection request, the network stack retries as per the configuration.
Conf Id, Value	Optional	12	0, 1 (default 0) 0 - enable 1 - disable	It specifies whether to broadcast SSID in beacon frames or not.
Conf Id, Value	Optional	13	1 to 65535 (default 3)	It specifies the dtim period in AP mode.
Conf Id, Value	Optional	14	1 to 65535 (default 3600)	It specifies the time-out interval when there is no activity from the connected nodes.
Conf Id, Value	Mandatory	25	Radio mode 1,2,3 1 - Active mode 2 - PS poll mode (default) 3 - IEEE PS poll mode	It specifies the radio mode during DHCP process.
Conf Id, Value	Mandatory	26	0xffffffff (default)	It specifies the lease period to be requested in DHCP discover message.
Conf Id, Value	Mandatory	27	2 seconds default	It specifies the time interval between successive DHCP retries.



NOTE: The L4 configuration parameters (L4 retry count and period) can be configured using ATS6/7 command. Refer to [3.7 Serial-to-WiFi Configuration](#), page 84.

Synchronous Response

[Table 247, page 263](#) describes the synchronous responses and remarks for NCM Configuration command.

Table 247 NCM Configuration Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid.

3.22.3 NCM Status Get

This command is used to get the status or the profile information of network connection manager.

Command Syntax

AT+NCMAUTO=? / ??

Parameter Description

[Table 249, page 264](#) describes the NCM Status Get parameters.

Table 248 NCM Status Get Parameters

Parameter	Optional/Mandatory	Value	Description
?	Mandatory	N/A	This parameter is used to get the status of network connection manager
??	Optional	N/A	This parameter is used to get the profile information of network connection manager

Example

This command displays the NCM status (NCM started or not) and the state in the following format.

```
NCM STARTED:<state>
```

3.22.4 NCM AP Configuration Enable

This command is used to enable the NCM AP configuration. The NCM AP parameters can be configured using the auto connect commands specified in section [2.2.1 Auto Connection, page 36](#). However, these commands are used for both station and limited AP mode. To distinguish the parameters for limited AP mode, the adapter provides a command.

Command Syntax AT+APCONF=<Enable>

Parameter Description

Table 249, page 264 describes the NCM AP Configuration Enable parameters.

Table 249 NCM AP Configuration Enable Parameters

Parameter	Optional/Mandatory	Value	Description
Enable	Mandatory	0 (default)	For Station mode
		1	For limited AP mode

Once it enabled, the parameters configured using commands in [2.2.1 Auto Connection, page 36](#) and [3.11 WiFi Security Configuration, page 115](#), goes to limited AP.

Values

Table 250, page 264 describes the adapter value settings.

Table 250 Adapter Value Settings for NCM AP Configuration Enable

Parameter	Description
SSID	GainSpanProv
Channel	1
Security	0 (open)
WEP Key	1234567890
WEP Key Index	1
WEP Key Length	5
WPA Phassphrase	GSDemo123
Beacon Interval	100
DHCP Server Enable	TRUE (1)
DNS Server Enable	TRUE (1)
IP Address	192.168.240.1
Subnet Mask	255.255.255.0
Gateway	192.168.240.1
DHCP Start IP Address	192.168.240.2
DNS Name	config.gainspan
User Name	admin
Pwd	admin

Synchronous Response

Table 251, page 265 describes the synchronous responses and remarks for NCM AP Configuration Enable command.

Table 251 NCM AP Configuration Enable Synchronous Responses

Responses	Remarks
OK	Success
ERROR:INVALID INPUT	If parameters are not valid. (Other than 0 and 1)

Example

AT+APCONF=1

3.22.5 Use Cases for NCM

This section provides examples for NCM in Limited AP and station modes.

Example for Limited AP Mode

AT+APCONF=1

OK

AT+WM=2

OK

AT+WAUTO=2, GainSpan,,1

OK

AT+NSET=192.168.51.1,255.255.255.0:192.168.51.1

OK

AT+NCMAUTO=1,1,0

OK

IP	SubNet	Gateway
192.168.67.53:255.255.225.0:192.168.51.1		
NWCONN-SUCCESS		

AT&w0

OK

AT+RESET

APP Reset-APP SW Reset

IP	SubNet	Gateway
192.168.51.1:255.255.255.0:192.168.51.1		
NWCONN-SUCCESS		

Example for Station Mode

AT+WAUTO=0, GainSpan

OK

AT+NAUTO=0,1,192.168.67.54,9000

OK

AT+NCMAUTO=0,1,1

OK

IP	SubNet	Gateway
192.168.67.53:255.255.225.0:192.168.67.1		
NWCONN-SUCCESS		

CONNECT 0

AT&W0

OK

3.23 Roaming

The adapter supports roaming which is used under the following conditions:

- APs have the Same SSID and same Security
 - WPA/WPA2 Enterprise security is not supported
- APs can be on different channels
- The S2W Adapter in Radio PS-Poll or Active Receive Mode
- Only RSSI is used. PER and other statistics are not used.

This feature will be bundled with Network Connection Manager (NCM) and roaming parameters are configured with the following AT command.

`AT+NCMAUTOCONF=<Param ID>, <Param Value>`

Parameter Description

Table 252, page 267 describes the Roaming parameters.

Table 252 Roaming Parameters

Parameter	Optional/Mandatory	Value	Description
Param ID	Mandatory	16	Roaming Feature Enabled/Disabled
Param Value		Disabled (default)	
Param ID	Mandatory	17	Lower RSSI Threshold
Param Value		70db (default)	
Param ID	Mandatory	18	Higher RSSI Threshold
Param Value		50db (default)	
Param ID	Mandatory	19	Time between Background Scans
Param Value		1000ms (default)	
Param ID	Mandatory	20	Number of Times Low Threshold is crossed before roaming trigger is enabled - N1
Param Value		3 (default)	
Param ID	Mandatory	21	Maintain L3 - there is a common DHCP Server.
Param Value		Maintain L3 enabled (default)	
Param ID	Optional	22	Maintain L4 - L4 connection are not closed.
Param Value		Maintain L4 (0-disable and 1-enable) (default 0)	

Table 252 Roaming Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
Param ID	Optional	23	Maximum number of scans to find the AP to connect.
Param Value		ScanRetryCnt = 5 (default)	
Param ID	Optional	24	Delay after maximum number of scans. Configure the time in milliseconds.
Param Value		ScanPauseTime = 5000msec (default)	

3.24 Provisioning

3.24.1 Web Provisioning Start

This command is used to support provisioning through web pages.

Command Syntax

AT+WEBPROV=<user name>,<password>[,SSL Enabled,Param
StoreOption,idletimeout,ncmautoconnect, format version]

Parameter Description

Table 253, page 270 describes the Web Provisioning Server Start parameters.

Table 253 Web Provisioning Server Start Parameters

Parameter	Optional/Mandatory	Value	Description
user name	Mandatory	1-16 characters	<p>Any valid username in the range 1-16 characters for the web provisioning.</p> <p>The characters in a valid username can be any of the following:</p> <ul style="list-style-type: none">• Alphabets, numbers, alpha numeric, or special characters• Combination of alphabets, numbers, alpha numeric, and special characters• Blank space
password	Mandatory	1-16 characters	<p>Any valid password in the range 1-16 characters for the web provisioning.</p> <p>The characters in a valid password can be any of the following:</p> <ul style="list-style-type: none">• Alphabets, numbers, alpha numeric, or special characters• Combination of alphabets, numbers, alpha numeric, and special characters• Blank space
SSL Enabled	Optional	0,1 0: To start the web server without SSL. (Default) 1: To start the web server with SSL.	<p>It is required to load the server certificate and server key prior to starting the SSL enabled web server.</p> <p>The command to load the certificate is:</p> <pre>AT+TCERTADD=SSL_SERVER, 0, <Server certificate length>, 0</pre> <p>The command to load the key is:</p> <pre>AT+TCERTADD=SERVER_KEY, 0, <keylength>, 0 <ESC>W<data of size key length></pre> <p>The command to load root certificate is:</p> <pre>AT+TCERTADD=SSL_CA, <format>, <size>, <location></pre>

Table 253 Web Provisioning Server Start Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
ParamStoreOption	Optional	0 (default) 1 and 2	<p>This option selects the provisioned parameters' store location.</p> <p>0 - For sending the provisioned info to the serial interface (HOST)</p> <p>1 - For storing the provisioned info to the adapter profile</p> <p>2 - For performing both options above.</p> <p>The provisioned information sent to the serial host:</p> <p>SSID=<ssid></p> <p>CHNL=channel></p> <p>CONN_TYPE=<connType>/*BSS*/</p> <p>MODE=<mode>/*0 -> to 802.11b*/</p> <p>SECURITY=<security> (1-open, 2-wep, 3-wpa/wpa2 personal, 4-wpa/wpa2 enterprise)</p> <p>WEP_ID=<wepID></p> <p>WEP_KE=<wepkey></p> <p>PSK_PASS_PHASE=<pskPassPhrase></p> <p>DHCP_ENBL=<0/1></p> <p>STATIC_IP=<static IP address></p> <p>SUBNT_MASK=<subnet Mask></p> <p>GATEWAY_IP=<gateway></p> <p>AUTO_DNS_ENBL=<0 /1></p> <p>PRIMERY_DNS_IP=<primary DNS server IP></p> <p>SECNDRY_DNS_IP=<secondary DNS IP></p> <p>AP-SSID=<ssid></p> <p>AP-CHNL=<Channel></p> <p>AP-BEACON-INTRL=<interval> (100-1600)</p> <p>AP-SECURITY=<security> (1-open, 2-wep, 3-wpa/wpa2 personal, 4-wpa/wpa2 enterprise)</p> <p>AP-PSK_PASS_PHRASE=<passphrase></p> <p>AP-WEP-ID=<id> (1-4)</p> <p>AP-WEP-KEY=<wep key></p> <p>AP- STATIC_IP=<static IP address></p> <p>AP -SUBNT_MASK=<subnet Mask></p> <p>AP- GATEWAY_IP=<gateway></p> <p>AP-DHCPSRVR-ENABLE=<0/1></p> <p>AP-DHCPSRVR-STARTIP=<IP></p> <p>DHCPSRVR-NO-CONN=64</p> <p>AP-DNSSLRVR-ENABLE=1</p>

Table 253 Web Provisioning Server Start Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
ParamStoreOption	Optional	0 (default) 1 and 2	AP-DNS-DOMAIN-NAME=<dns name> NEW_USER_NAME=<new User Name> NEW_PASS=<new Password> WEP_AUTH_MODE=<Mode Value> (1- open, 2-shared) AP-WEP_AUTH_MODE=<Mode Value> (1- open, 2-shared)
idletimeout	Optional	120 seconds	HTTPS server starts a timer when a client connects to it. It closes the connection with client when there is no communication within the specified idletimeout time frame.
ncmautoconnect	Optional	0, 1	0 - Do not start the NCM 1 - Start the NCM after storing the parameters
format version	Optional	0,1	0: Prints the GS1011 compatible information 1: Prints the extra information which is not compatible with GS1011

Example

```
AT+NSET=192.168.17.111,255.255.255.0,192.168.17.1
OK
```

```
AT+WM=2
OK
```

```
AT+WA=GainSpanDemo,,11
IP           SubNet           Gateway
192.168.17.111:255.255.255.0:192.168.17.1
OK
```

```
AT+DHCPSRVR=1
OK
```

```
AT+WEBPROV=admin,admin,,1,,1
OK
```

Prior to issuing this command the adapter should be in an ad hoc or limited AP network with a valid IP address. Upon reception of this command the adapter starts a web server.

Once the adapter returns the success response (“OK”), the user can open a webpage on the PC (where the ad hoc network was created) with the IP address of the adapter and the HTTP client application (e.g. Internet Explorer).

If the adapter is configured as limited AP, the DHCP and DNS server should be started prior to issuing this command. Once the adapter returns the success response (“OK”), the user can open a web page on the PC or smart phone that is connected to the limited AP.

User can configure both L2 and L3 level information on the provisioning web pages.
Submit button stores all the configured information in the adapter and logout/boot button presents all provisioned information to the serial host and resets the adapter.

Synchronous Response

Table 254, page 274 describes the synchronous responses and remarks for Web Provisioning Start command.

Table 254 Web Provisioning Start Synchronous Responses

Responses	Remarks
OK	Success
ERROR: INVALID INPUT	If parameters are not valid.

3.24.2 Web Provisioning Stop

This command is used to stop Web provisioning. This command is typically done at the manufacturing line in the factory. This command can be done only once. There is no command to delete the Logo.

Command Syntax AT+WEBPROVSTOP**Synchronous Response**

Table 255, page 274 describes the synchronous responses and remarks for Web Provisioning Stop command.

Table 255 Web Provisioning Stop Synchronous Responses

Responses	Remarks
OK	Success
ERROR	If command is issued without starting web provisioning using AT+WEBPROV command.

3.24.3 HTTPD Redirection

This command is used to add the redirection URL on the adapter.

Command Syntax AT+NURIREDIR=<URL>**Parameter Description**

Table 256, page 274 describes the HTTPD Redirection parameters.

Table 256 HTTPD Redirection Parameters

Parameter	Optional/Mandatory	Value	Description
URL	Mandatory	Max URL length is 64 bytes	URL is the address of the redirection page.

3.24.4 Group Provisioning

Group provisioning mode supports to provision a group of devices together. In this mode, the GS module acts as Limited AP with the following default settings:

- SSID with a prefix and MAC ID
 - Prefix: GS_PROV
 - MAC ID: Last 6 digits of MAC ID
- Example: If MAC ID is 00:1d:c9:23:1d: 3c, then the SSID will be GS_PROV_231d3c.
- Open security in channel 1
- HTTPS server
- mDNS

Prerequisites

For GS module to work in Group Provisioning mode, it is mandatory to enable the following options in SDK builder:

- NCM AUTOSTART
- mDNS
- HTTPS Server
- DHCP Server



NOTE: If Group Provisioning mode is enabled, then NCM AUTOSTART, mDNS, HTTPS Server are enabled by default. Otherwise, this has to be enabled manually.

Procedure to Support Group Provisioning

Using SDK Builder

To enable Group Provisioning mode using SDK Builder,

1. Access SDK Builder, and select **Group Provisioning** under **Provisioning** tab.
2. Click on the '+' symbol to view the configuration parameters for Group Provisioning.
3. Configure the following parameters as per requirement.

Table 257 Group Provisioning Parameters

Parameter	Optional/Mandatory	Value	Description
Regulatory Domain	Optional	<ul style="list-style-type: none"> • FCC • ETSI • TELEC 	It specifies the regulatory domain used based on User preference.
Mode	Optional	bgn Mixed	Mode bgn Mixed is being used in Group provisioning.
Channel	Optional	1-11	It specifies the channel number for the Android device.
Beacon Interval	Optional	50-1500 Unit: milliseconds	It indicates the interval at which the Limited AP broadcasts the beacon frames. Note: Beacon Interval range of 50 is recommended in poor reception.
Broadcast SSID	Optional	<ul style="list-style-type: none"> • Enable • Disable 	It specifies whether broadcasting SSID is enabled or disabled.
Security	Optional	Open	Security type Open with no authentication is being used in Group provisioning.
Stations Supported	Optional	1-64	It specifies the number of stations supported during Group provisioning.

Using AT Commands from Host MCU To enable Group Provisioning using AT commands from Host MCU,

1. Load SSL certificates using the following commands:

```
AT+TCERTADD=SSL_SERVER,0,670,0
AT+TCERTADD=SSL_CA,0,760,0
AT+TCERTADD=SSL_KEY,0,609,0
```

For more information about AT+TCERTADD command, refer [3.11.10 EAP Time Validation, page 127](#).

2. Stop the NCM AUTO mode by executing the following command:

```
AT+NCMAUTO=1,0,0,0
AT+WD
```

3. Configure the GS module to support Group provisioning mode by executing the following command:

```
AT+WM=6
```

4. Start the NCM AUTO by executing the following command:

```
AT+NCMAUTO=1,1,0,0
```

5. Start the Group provisioning mode using the Android application.

3.25 RF Tests

3.25.1 RF Tests for GS2011M

3.25.1.1 RF Test Mode Start for GS2011M

This command is used to enable the radio test mode.

Command Syntax AT+WRFTESTSTART

3.25.1.2 RF Test Mode Stop for GS2011M

This command is used to disable the radio test mode.

Command Syntax AT+WRFTESTSTOP

3.25.1.3 Asynchronous Frame Transmission for GS2011M

This command is used to enable the frame transmission. This command enables the asynchronous data transmission with the parameters configured. After issuing this command the transmission will go with the default payload.

Command Syntax AT+WFRAMETXTEST=<Channel>,<BandWidth>,<NumFrames>,<FrameLen>,<TxRate>,<TxPower>,<DestAddr>,<Bssid>,<HtEnable>,<GuardInterval>,<GreenField>,<PreambleType>,<QosEnable>,<AckPolicy>,<Scrambler>,<AifsnVal>,<Antenna>,<ccaBypass>

Parameter Description

Table 258, page 277 describes the Asynchronous Frame Transmission parameters.

Table 258 Asynchronous Frame Transmission Parameters

Parameter	Optional/Mandatory	Value	Description
Channel	Mandatory	1-14	The channel on which the data to be sent (1-14).
BandWidth	Mandatory	0,1	The values can be 0 (20MHz) or 1 (40MHz).
Note: The GS2000 currently supports 20MHz operation.			
NumFrames	Mandatory	1-65535	The number of asynchronous frames to be sent (1-65535).
Note: for continuous transmission, configure this parameter with the value 99. Once configured in continuous transmission mode, to come out of this mode, stop the test mode and start the test mode again (i.e., AT+WRFTESTSTOP, AT+WRFTESTSTART).			
FrameLen	Mandatory	32 to 1500	The length of the payload.

Table 258 Asynchronous Frame Transmission Parameters

Parameter	Optional/Mandatory	Value	Description
TxRate	Mandatory	N/A	The rate at which the data need to be sent. See Table 259, page 278 .
Note: This also depends on the HtEnable field. If HtEnable bit is set, the configured TxRate is taken as MCS index, otherwise legacy rate.			
TxPower	Mandatory	0 to 27	The value of this parameter can range from 0 to 27. Where 27 is the index corresponding to the maximum TxPower GS2000 will support.
DestAddr	Mandatory	N/A	The MAC address of the node target to reach.
BSSID	Mandatory	N/A	The MAC address of any arbitrary AP, which will be the source MAC address.
HtEnable	Mandatory	0 1	High throughput disabled High throughput enabled
GuardInterval	Mandatory	1 0	Short guard interval Long guard interval
GreenField	Mandatory	0 1	11n disabled 11n only
PreambleType	Mandatory	0 1	short long
QosEnable	Mandatory	0	Enable QoS
AckPolicy (Debug parameter)	Mandatory	4	N/A
Scrambler (Debug parameter)	Mandatory	0 1	OFF ON
AifsVal	Mandatory	N/A	N/A
Antenna	Mandatory	N/A	N/A
ccaBypass	Mandatory	N/A	N/A

[Table 259, page 278](#) describes the Asynchronous Frame Transmission Data Rates for GS2011M.

Table 259 Asynchronous Frame Transmission Data Rates

TxRate	HtEnable	Data Rate (Mbps)
1	0	1
2	0	2
5	0	5.5
11	0	11

Table 259 Asynchronous Frame Transmission Data Rates

TxRate	HtEnable	Data Rate (Mbps)
6	0	6
9	0	9
12	0	12
18	0	18
24	0	24
36	0	36
48	0	48
54	0	54
0	1	MCS0
1	1	MCS1
2	1	MCS2
3	1	MCS3
4	1	MCS4
5	1	MCS5
6	1	MCS6
7	1	MCS7

Example

```
AT+WFRAMETXTEST=1,0,50000,1000,11,16,00:11:22:33:44:55,00
:50:c2:5e:10:99,0,0,0,0,0,4,0,2,0,1
```



NOTE: Check the wireless sniffer to see if the frames are on air.

3.25.1.4 Asynchronous Frame Reception Start for GS2011M

The command is used to enable the asynchronous frame reception.

Command Syntax AT+WRXTEST=<Channel>,<BandWidth>,<RxFrameTypeFilter>,<RxAddrFilter>,<Antenna>

Parameter Description

Table 260, page 280 describes the Asynchronous Frame Reception Start parameters.

Table 260 Asynchronous Frame Reception Start Parameters

Parameter	Optional/Mandatory	Value	Description
Channel	Mandatory	1 to 14	The channel on which the data is to be sent (1-14).
BandWidth	Mandatory	0, 1	The values can be 0 (20MHz) or 1 (40MHz).
Note: Currently GS2011M supports only 20MHz operation.			
RxFrameTypeFilter	Mandatory	32-bit	This is a 32-bit variable, where each bit corresponds to one type of packet filter.
RxAddrFilter	Mandatory	N/A	The MAC address of the Destination node.
Note: The Rx filter is based on destination address. For PER test, transmit from another GS2000 or some other source specifying the destination address and set up the receiver to receive frames only destined to its address. Receiver can be set up to receive all frames by setting filter to zero but that's not useful for PER because you don't know how many frames were sent. Source address based filtering is not supported.			
Antenna	N/A	N/A	Not supported

Example

AT+WRXTEST=6,0,4294930106,00:11:22:33:44:55,0



NOTE: This will receive frames with MAC address 00:11:22:33:44:55.



NOTE: RxFrameTypeFilter is set to 0xFFFF6EBA (42949301206) to receive unicase directed management and data frames. This is setup to receive all kinds of frames destined to the receiver mode.

From Tx side, transmit frames with MAC address specified in Rx command. Use the following command:

```
AT+WFRAMETXTEST=6,0,10000,1000,24,16,00:11:22:33:44:55,00  
:33:44:55:66:77,0,0,0,0,0,4,0,2,0,1
```

```
AT+WRXTEST=1,0,0,00:11:22:33:44:55,0
```

AT+WRXTEST=1,0, 536870912,00:11:22:33:44:55,0 - To filter
FCS Fail packets

Issue the AT+WRXSTOP to find the Rx statics details on the Tera Term.

3.25.1.5 Asynchronous Frame Reception Stop for GS2011M

This command is used to stop any of the RF reception.

Command Syntax

AT+WRXSTOP

Example

When the command is executed it stops the frame reception and displays the PER stats:

```
AT+WRXTEST=6, 0, 4294930106, 00:11:22:33:44:55, 0
OK

AT+WRXSTOP
No of packets received = 9613
No of bytes received = 9613000
No of packets received with CRC Errors = 1432
No of packets received with Security Errors = 0
No of duplicate packets received = 0
No of header errors received = 58
Average RSSI of the received packets = -49
No of packets received at 1M and Long Preamble = 0
No of packets received at 2M and Long Preamble = 0
No of packets received at 5M and Long Preamble = 0
No of packets received at 11M and Long Preamble = 0
No of packets received at 2M and Short Preamble = 0
No of packets received at 5M and Short Preamble = 0
No of packets received at 11M and Short Preamble = 0
No of packets received at 6M = 0
No of packets received at 9M = 0
No of packets received at 12M = 0
No of packets received at 18M = 0
No of packets received at 24M = 9613
No of packets received at 36M = 0
No of packets received at 48M = 0
No of packets received at 54M = 0
No of packets received at respective MCS Index with Short
GI=00000000
No of packets received at respective MCS Index with Long
GI=00000000
```



NOTE: FCS and header errors are on all received frames. For PER calculation, compare the total filtered received frames with the total sent frames. You cannot use FCS and header errors for address filtering because only good frames are considered.

3.25.1.6 Asynchronous Frame Transmission (TX99 mode) for GS2011M

This command is used to enable TX99 mode.



NOTE: Issue AT+WRFTESTSTART command before issuing the FrameTX test or the TX99 test commands; otherwise a WLAN exception/reset will occur.

Command Syntax

```
AT+WTX99TEST=<Channel>,<BandWidth>,<NumFrames>,<FrameLen>
,<TxRate>,<TxPower>,<DestAddr>,<Bssid>,<GuardInterval>,
<GreenField>,<Antenna>,<Cca>,<Agc>,<ContPreambleMode>,
<Spreader>,<Scrambler>,<Preamble>,<PreambleType>,
<TestPatternType>,<PhyTestTxRate>,<ModeSelect>
```

Usage

This command enables the asynchronous data transmission with the parameters configured.

Parameter Description

Table 261, page 283 describes the Asynchronous Frame Transmission (TX99 mode) parameters.

Table 261 Asynchronous Frame Transmission Parameters

Parameter	Optional/Mandatory	Value	Description
Channel	Mandatory	1 to 14	The channel on which the data is to be sent (1-14).
BandWidth	Mandatory	0, 1	The values can be 0 (20MHz) or 1 (40MHz).
Note: Currently the GS2000 supports only 20MHz operation.			
NumFrames	Mandatory	1-65535	The number of asynchronous frames to be sent (1-65535).
Note: For continuous transmission, configure this parameter with the value 99.			
FrameLen	Mandatory	32-1500	The length of the payload.
TxRate	Mandatory	0 to 7	<ul style="list-style-type: none"> • Non HT Rates - 0 • Ht Rate - 0 to 7 (MCS Index)
Note: Use PhyTestTxRate and ModeSelect fields to change the transmission rate.			
TxPower	Mandatory	0 to 27	The value of this parameter can range from 0 to 27. Where 27 is the index corresponding to Maximum TxPower GS2000 will support.
DestAddr	Mandatory	N/A	The MAC address of the node targeted to reach.
BSSID	Mandatory	N/A	The MAC address of any arbitrary AP, which will be the source MAC address.

Table 261 Asynchronous Frame Transmission Parameters

Parameter	Optional/Mandatory	Value	Description
GuardInterval	Mandatory	0, 1 • 0 - Short guard interval • 1 - Long guard interval	It specifies the guard interval.
GreenField	Mandatory	0, 1 • 0 - 11n disabled • 1 - 11n only	It specifies whether to enable or disable 11n.
Antenna	Optional	N/A	It specifies the antenna used.
Cca	Optional	0,1 • 0 - Normal mode • 1 - Removes the control of CCA module on the receiver state machine in PHY	It specifies whether to enable normal mode or remove the control of CCA module on the receiver state machine in PHY.
Agc	Mandatory	0, 1 • 0 - Normal mode • 1 - Removes the control of AGC module on the receiver state machine in PHY	It allows to enable normal mode or remove the control of AGC module on the receiver state machine in PHY.
ContpreambleMode	Mandatory	0, 1 • 0 - Disable Continuous Preamble Mode • 1 - Enable Continuous Preamble Mode	It allows to enable or disable the continuous preamble mode.
Spreader	Mandatory	0, 1 • 0 - Spreader is OFF • 1 - Spreader is ON	It allows to enable or disable Spreader.
Scrambler	Mandatory	0, 1 • 0 - Scrambler is OFF • 1 - Scrambler is ON	It allows to enable or disable Scrambler.
Preamble	Mandatory	0, 1 • 0 - Normal mode • 1 - Disables short and long preamble in the transmitter	It allows to enable normal mode or disable short and long preamble in the transmitter.
PreambleType	Mandatory	0, 1 • 0 - Short Preamble • 1 - Long Preamble	It specifies the Preamble type.

Table 261 Asynchronous Frame Transmission Parameters

Parameter	Optional/Mandatory	Value	Description
TestPatternType	Mandatory	<ul style="list-style-type: none"> • 000 (0)- All 1's • 001 (1)- All 0's • 010 (2)- Alternate 1's and 0's • 011 (3)- PN15 random sequence • 100 (4)- PN9 random sequence • 111 (7)- PN7 random sequence 	It specifies the type of test pattern to be used.
PhyTestTxRate	Mandatory	0 to 7	<p>It specifies the PHY test transmission rates.</p> <p>The rates differ depending on the ModeSelect.</p>
ModeSelect	Mandatory	0, 1, 2 <ul style="list-style-type: none"> • 0 - 11g mode • 1 - 11b mode • 2 - 11n mode 	It specifies the mode to be used.

Table 262, page 286 describes ModeSelect, TxRate, and PHY test transmit rates for corresponding Data rates (TX99 mode).

Table 262 ModeSelect, TxRate, PHY test transmit rates for corresponding Data rates (TX99 mode)

Data Rate (Mbps)	ModeSelect	Mode	TxRate	PhyTestTxRate
1	1	802.11b	0	0
2	1		0	1
5.5	1		0	2
11	1		0	3
6	0	802.11g	0	3
9	0		0	7
12	0		0	2
18	0		0	6
24	0		0	1
36	0		0	5
48	0		0	0
54	0		0	4
MCS0	2	802.11n	0	0
MCS1	2		1	1
MCS2	2		2	2
MCS3	2		3	3
MCS4	2		4	4
MCS5	2		5	5
MCS6	2		6	6
MCS7	2		7	7

**Example for Mode
802.11b**

To support data rate of 11 Mbps, configure the **ModeSelect** parameter to **1**, **TxRate** parameter to **0**, and **PhyTestTxRate** to **3**.

```
AT+WTX99TEST=1,0,25000,1000,0,20,00:11:22:33:44:55,00:50:  
c2:5e:10:99,0,0,0,0,1,0,1,1,0,1,3,1
```

Check the wireless sniffer to see the frame on air. Though some sniffers capture these packets, the best way to validate these packets will be using litepoint device.

**Example for Mode
802.11g**

To support data rate of 18 Mbps, configure the **ModeSelect** parameter to **0**, **TxRate** parameter to **0**, and **PhyTestTxRate** to **6**.

```
AT+WTX99TEST=1,0,25000,1000,0,20,00:11:22:33:44:55,00:50:  
c2:5e:10:99,0,0,0,0,1,0,1,1,0,1,3,1
```

Example for Mode 802.11n To support data rate of MCS5, configure the **ModeSelect** parameter to **2**, **TxRate** parameter to **5**, and **PhyTestTxRate** to **5**.

```
AT+WTX99TEST=1,0,25000,1000,0,20,00:11:22:33:44:55,00:50:  
c2:5e:10:99,0,0,0,0,1,0,1,1,0,1,3,1
```

The following table provides examples of Tx99 mode command for corresponding Data rates.

Table 263 Examples for Asynchronous Frame Transmission (TX99 mode)

Data Rate (Mbps)	Example
1	AT+WTX99TEST=1,0,99,1000,0,18,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,1,0,1,1,0,3,0,1
2	AT+WTX99TEST=1,0,99,1000,0,8,00:11:22:33:44:55,00:50:c 2:5e:10:99,0,0,0,0,1,0,1,1,1,0,3,1,1
5.5	AT+WTX99TEST=1,0,99,1000,0,14,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,1,0,1,1,1,0,3,2,1
11	AT+WTX99TEST=1,0,99,1000,0,11,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,1,0,1,1,1,0,3,3,1
6	AT+WTX99TEST=1,0,99,1000,0,27,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,3,0
9	AT+WTX99TEST=1,0,99,1000,0,27,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,7,0
12	AT+WTX99TEST=1,0,99,1000,0,27,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,2,0
18	AT+WTX99TEST=1,0,99,1000,0,27,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,6,0
24	AT+WTX99TEST=1,0,99,1000,0,26,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,1,0
36	AT+WTX99TEST=1,0,99,1000,0,25,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,5,0
48	AT+WTX99TEST=1,0,99,1000,0,24,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,0,0
54	AT+WTX99TEST=1,0,99,1000,0,19,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,4,0
MCS0	AT+WTX99TEST=1,0,99,1000,0,27,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,0,2
MCS1	AT+WTX99TEST=1,0,99,1000,1,27,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,1,2
MCS2	AT+WTX99TEST=1,0,99,1000,2,27,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,2,2
MCS3	AT+WTX99TEST=1,0,99,1000,3,27,00:11:22:33:44:55,00:50: c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,3,2

Table 263 Examples for Asynchronous Frame Transmission (TX99 mode)

Data Rate (Mbps)	Example
MCS4	AT+WTX99TEST=1,0,99,1000,4,25,00:11:22:33:44:55,00:50:c2:5e:10:99,0,0,0,0,0,0,0,0,0,3,4,2
MCS5	AT+WTX99TEST=1,0,99,1000,5,24,00:11:22:33:44:55,00:50:c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,5,2
MCS6	AT+WTX99TEST=1,0,99,1000,6,20,00:11:22:33:44:55,00:50:c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,6,2
MCS7	AT+WTX99TEST=1,0,99,1000,7,16,00:11:22:33:44:55,00:50:c2:5e:10:99,0,0,0,0,0,0,0,0,0,0,3,7,2

3.25.1.7 Asynchronous Frame Transmission (TX100 mode) for GS2011M

This command is used to enable the TX100.

Command Syntax

```
AT+WTX100TEST=<Channel>,<BandWidth>,<TxPower>,<Antenna>,<  
Cca>,<Agc>,<ContPreambleMode>,<Spreader>,<Scrambler>,<Pre  
amble>,<PreambleType>,<TestPatternType>,<PhyTestTxRate>,<  
ModeSelect>
```

Parameter Description

Table 264, page 289 describes the Asynchronous Frame Transmission (TX100 mode) parameters.

Table 264 Asynchronous Frame Transmission (TX100 mode)

Parameter	Optional/Mandatory	Value	Description
Channel	Mandatory	1-14	The channel on which the data to be sent.
BandWidth	Mandatory	0, 1	The values can be 0 (20MHz) or 1 (40MHz).
Note: Currently the GS2000 supports only 20MHz operation.			
TxPower	Mandatory	0-27	The value of this parameter can range from 0 to 27. Where 27 is the index corresponding to Maximum TxPower GS2000 will support.
Antenna	Optional	0	Antenna
Cca	Mandatory	0,1	<ul style="list-style-type: none"> • 0 - Normal mode • 1 - Removes the control CCA module on the receiver state machine in PHY
Agc	Mandatory	0,1	<ul style="list-style-type: none"> • 0 - Normal mode • 1 - Removes the control of AGC module on the receiver state machine in PHY
ContpreambleMode	Mandatory	0,1	<ul style="list-style-type: none"> • 0 - Disable Continuous Preamble Mode • 1 - Enable Continuous Preamble Mode
Spreader	Mandatory	0,1	<ul style="list-style-type: none"> • 0 - Spreader is OFF • 1 - Spreader is ON
Scrambler	Mandatory	0,1	<ul style="list-style-type: none"> • 0 - Scrambler is OFF • 1 - Scrambler is ON
Preamble	Mandatory	0,1	<ul style="list-style-type: none"> • 0 - Normal mode • 1 - Disables short and long preamble in the transmitter
PreambleType	Mandatory	0,1	<ul style="list-style-type: none"> • 0 - Short Preamble • 1 - Long Preamble

Table 264 Asynchronous Frame Transmission (TX100 mode) (Continued)

Parameter	Optional/Mandatory	Value	Description
TestPatternType	Mandatory	0,1	Selects the test pattern to be transmitted. <ul style="list-style-type: none"> • 0 - All 1s • 1 - All 0s
PhyTestTxRate	Mandatory	0 to 7	The rate will differ depending on the ModeSelect (see Table 265, page 290).
ModeSelect	Mandatory	0 to 2	<ul style="list-style-type: none"> • 0 - 11g mode • 1 - 11b mode • 2 - 11n mode

[Table 265, page 290](#) describes the PHY Test Transmit Rates (TX100 mode).

Table 265 PHY Test Transmit Rates (TX100 mode)

Mode Select	PhyTestTxRate	Data Rate (Mbps)
1	0	1
1	1	2
1	2	5.5
1	3	11
0	3	6
0	7	9
0	2	12
0	6	18
0	1	24
0	5	36
0	0	48
0	4	54
2	0	MCS0
2	1	MCS1
2	2	MCS2
2	3	MCS3
2	4	MCS4
2	5	MCS5
2	6	MCS6
2	7	MCS7

Example

```
AT+WTX100TEST=1,0,16,0,0,1,0,0,1,1,0,1,3,1
```



NOTE: Special equipment may need to be setup in order to observe the signals.

3.25.1.8 Carrier Wave Transmission for GS2011M

This command is used to enable the carrier wave transmission.

Command Syntax

AT+WCARWAVTEST=<Channel>,<BandWidth>,<TxPower>,<Antenna>,<CustomWavePeriod>

Parameter Description

Table 266, page 291 describes the Carrier Wave Transmission parameters.

Table 266 Carrier Wave Transmission Parameters

Parameter	Optional/Mandatory	Value	Description
Channel	Mandatory	1-14	The channel on which the data to be sent.
BandWidth	Mandatory	0,1	The values can be 0 (20MHz) or 1 (40MHz).
Note: Currently the GS2000 supports only 20MHz operation.			
TxPower	Mandatory	0-27	The value of this parameter can range from 0 to 27. Where 27 is the index corresponding to Maximum TxPower GS2000 will support.
Antenna	Optional	N/A	Antenna
CustomWavePeriod	Optional	N/A	The period in which the carrier wave is transmitted.

Example

AT+WCARWAVTEST=11,0,27,0,2

3.26 Miscellaneous

3.26.1 Enhanced Asynchronous Notification

This command is used to support enhanced asynchronous notification method.

Command Syntax AT+ASYNMSGFMT=n

Parameter Description

Table 267, page 292 describes the Enhanced Asynchronous Notification parameters.

Table 267 Enhanced Asynchronous Notification Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	0 (default) 1	Disable this feature Enable this feature
			Enabling this feature results with all asynchronous message going to the serial interface with a header. Also during these asynchronous message transfer S2W adapter makes the GPIO 19 high. Node Start Up Handling.
Format			The asynchronous message format is as shown: <ESC><TYPE><SUBTYPE><LENGTH><MESSAGE>
			<ESC> Escape
			TYPE Type of message and the length is one byte. For asynchronous message, it is 0x41 (ASCII value A)
			SUBTYPE Message subtype and the length of this field is: <ul style="list-style-type: none">One byte when the value of this byte is one of the values from 0 to E.Two bytes when the value of this byte is F where the first byte and the next byte is read and interpreted as per the table in 2.7.1 Enhanced Asynchronous Messages, page 55.
			LENGTH Length of the asynchronous message in hex. This field length is 2 bytes. See 2.7.1 Enhanced Asynchronous Messages, page 55 .
			MESSAGE Exact asynchronous message as string.

Synchronous Response

Table 268, page 292 describes the synchronous responses and remarks for Enhanced Asynchronous command.

Table 268 Enhanced Asynchronous Notification Synchronous Responses

Responses	Remarks
OK	Success
ERROR: INVALID INPUT	If parameters are not valid. (If n value is other than 0 and 1)

**Example 1-
Asynchronous
message CONNECT
(When GS node acts
as a TCP server)**

```
AT+WA=GainSpanDemo
IP           SubNet       Gateway
192.168.1.99:255:255:255.0:192.168.1.1
OK

AT+NDHCP=1
IP           SubNet       Gateway
192.168.17.4:255:255:255.0:192.168.17.1
OK

AT+NSTCP=8000
CONNECT 0
OK

AT+ASYNCMMSGFMT=1
OK
11eCONNECT0 1 192.168.17.250090
```

3.26.2 Set System Time

This command is used to set the adapters system time to the time specified as the parameters and returns the standard command response. The adapter expects either one of the time parameters.

Command Syntax

AT+SETTIME=[<dd/mm/yyyy>,<HH:MM:SS>], [System time in milliseconds since epoch(1970)]

Usage

This command does not take care of the day light savings. The reference will be with respect to UTC/GMT.

3.26.3 Set System Time Using SNTP

This command is used to set the adapter system time using the SNTP.

Command Syntax

AT+NTIMESYNC= <Enable>,<Server IP>,<Timeout>,<Periodic>,[<frequency>]

Usage

This command returns OK/ ERROR/ INVALID INPUT/SNTP Busy. The time set by this command can be verified using the AT+GETTIME=? command. SNTP Busy status is sent if previous time synchronization is not finished.



NOTE: The time set will be UTC/GMT.

Parameter Description

Table 269, page 294 describes the Set System Time Using SNTP parameters.

Table 269 System Time Using SNTP Parameters

Parameter	Optional/Mandatory	Value	Description
Enable	Mandatory	0,1	<ul style="list-style-type: none">• 0 - stops the time sync• 1 - starts the time sync using SNTP
Server IP	Mandatory	N/A	SNTP server IP
Timeout	Mandatory	N/A	The time to wait for the server response (in seconds).
Periodic	Mandatory	0,1	The time sync to be done one time or periodically. <ul style="list-style-type: none">• 0 - one time• 1 - periodic
Frequency	Optional	N/A	If the periodic flag is set, the time difference between each time sync (in seconds).

3.26.4 Get System Time

This command is used to send the current system time in formatted and in milliseconds since epoch (1970) followed by the standard command response to the serial interface. The time format comes on the serial interface as follows:

=<dd/mm/yyyy>, <HH:MM:SS>

The system time is in milliseconds since epoch (1970).

Command Syntax

AT+GETTIME=?

3.26.5 GPIO Out HIGH/LOW

This command is used to set/reset the GPIO ‘GPIO-NO’ pin level to high or low as per the SET/RESET parameter.

Command Syntax

AT+DGPIO=<GPIO-NO>, <SET/RESET (0/1)>



NOTE: Only the GPIO pins which are not mixed with any used IOs, like UART/SPI, etc. that can be set high/low with this command.

Parameter Description

Table 270, page 295 describes the GPIO Out HIGH/LOW parameters.

Table 270 GPIO Out HIGH/LOW Parameters

Parameter	Optional/Mandatory	Value	Description
GPIO 4	Optional	4	General Purpose Input Output 4
GPIO 5	Optional	5	General Purpose Input Output 5
GPIO 6	Optional	6	General Purpose Input Output 6
GPIO 7	Optional	7	General Purpose Input Output 7
GPIO 9	Optional	9	General Purpose Input Output 9
GPIO 20	Optional	20	General Purpose Input Output 20
GPIO 21	Optional	21	General Purpose Input Output 21
GPIO 29	Optional	29	General Purpose Input Output 29
GPIO30	Optional	30	General Purpose Input Output 30
GPIO31	Optional	31	General Purpose Input Output 31

3.26.6 Version

This command is used to return version information.

Command Syntax AT+VER=?

- Command Response**
- Serial-to-WiFi version
 - GainSpan Embedded Platform Software version
 - WLAN firmware version

Example 1 AT+VER=?

```
S2W APP VERSION=5.1.4
S2W GEPS VERSION=5.1.4
S2W WLAN VERSION=5.1.4
OK
```

The command to get more details of the S2W version.

```
AT+VER=??
```

Command Response This command returns more information along with the above response of the S2W binary followed by the standard command response to the serial host.

- Serial-to-WiFi version
- GainSpan Embedded Platform Software version
- WLAN firmware version
- Serial-to-WiFi binary type as specified in SDK builder
- Serial-to-WiFi Release type which can be GA or Beta
- Build time
- Build date
- WLAN firmware extension version
- Application firmware extension version
- WLAN feature bitmap
- GEPS firmware extension version
- Module flash ID with storage capacity

Example 2 AT+VER=??

```
S2W APP VERSION=5.1.4
S2W GEPS VERSION=5.1.4
S2W WLAN VERSION=5.1.4
S2W BIN TYPE=5_1_4_Unsolicited_Tx
S2W RELEASE TYPE=GA
BUILD TIME=03:33:28
```

```
BUILD DATE=Jan 27 2015
WLAN EXT VERSION=5
S2W APP EXT VERSION=1
WLAN FEAT BMAP=0000000000000007
GEPS EXT VERSION=1
FLASH ID=0x000020c2:MICRONIX-4MB
OK
```

3.26.7 Ping for IPv4

This command is used to send the device a *ping* to the remote machine specified by the IPv4 address.

Command Syntax

AT+PING=<Ip>, [[<Trails>], [<timeout>], [<Len>], [<TOS>], [<TTL>], [<PAYLOAD>]]

Parameter Description

Table 271, page 298 describes the Ping for IPv4 parameters.

Table 271 Ping for IPv4 Parameters

Parameter	Optional/Mandatory	Value	Description
IP	Mandatory	N/A	The IP address of the server to which the command is directed.
Trails	Mandatory	0 (default)	This indicates the number of <i>ping</i> requests to send. In this case, <i>ping</i> will continue until terminated.
Timeout	Mandatory	3000 (default)	This is the timeout in milliseconds for each <i>ping</i> response to come after it sends out a <i>ping</i> request. The valid range is 1000-99000.
Len	Mandatory	56 (default)	The length of the <i>ping</i> packet. The valid range is 0 to 1024. The packet length is fixed for the GS2000M.
TOS	Mandatory	0 (default)	This is the type of service. The valid range is 0-99.
Note: Packet length is fixed in GS2000.			
TTL	Mandatory	30 (default)	This is the time to live. The valid range is 0-255.
Payload	Mandatory	0 to 16	This is the data to be sent in each <i>ping</i> packet. The payload length should be in the range 0-16. The payload may contain valid alphanumeric characters (0-9, A-F).
Note: To terminate a <i>ping</i> sequence, issue the <ESC>C			

3.26.8 Reset

This command is used to reset the adapter.

Command Syntax AT+RESET

Usage This command forcefully reset the adapter and comes out with a fresh boot message APP Reset-APP SW Reset

3.26.9 WLAN Statistics for GS2000

This command is used to request the GS2011M to send the statistics that it maintains. Including Rx, Tx, and encryption errors. Wireless statistics counters silently wrap. It is the responsibility of the host to read the counters periodically before the wrap loses information.

Command Syntax AT+WLANSTATS

Usage When the statistics are sent to the host, the GS2011M clears them so that a new set of statistics are collected for the next report.

This command returns the statistics counters in the following order separated. Some fields have multiple values and for that failure and success counts are separated by a comma. Each set is delimited by “:” character.

Table 272, page 299 describes GS2000 WLAN TX Statistic counters.

Table 272 GS2000 WLAN TX Statistic Counters

WLAN Statistic Counters	Description
itxs	TX Success
itxto	TX Timeout
itxf	TX Failed
wep40	WEP-40 encrypted
wep104	WEP-104 encrypted
tkip	TKIP encrypted
ccmp	CCMP encrypted
unencryp	Not encrypted
ukencryp	Unknown encryption
leg	Legacy frames
ht20l	HT-LongGl-20MHz
ht20s	HT-Shrtl-20MHz
ht40l	HT-LongGl-40MHz
ht40s	HT-ShrtGl-40MHZ
mcs32s	MCS-32 ShortGl
mcs32l	MCS-32 LongGl

Table 272 GS2000 WLAN TX Statistic Counters (Continued)

WLAN Statistic Counters	Description
probersp	Probe response
proberreq	Probe request
mc_data	Multicase data
uc_data	Unicast data
qos_uc_data	Unicast QoS data
qos_mc_data	Multicast QoS data
amsdu_uc_data	Unicast AMSDU data
amsdu_mc_data	Multicast AMSDU data
ampdu_uc_data	Unicast AMPDU data
ampdu_mc_data	Multicast AMPDU data
oth_mgmt	Other management
oth	Other frames
ctrl	Control frames
retries	Retries
multiple_retries	Multiple retries
fragments	Fragments

Table 273, page 300 describes GS2000 WLAN RX Statistic counters.

Table 273 GS2000 WLAN RX Statistic Counters

WLAN Statistic Counters	Description
irx0	Invalid
irxf	FCS Failure
irxs	RX Successful
irxd	Duplicate Detected
irxmf	MIC Failed
irxkf	Key Failed
irxicvf	ICV Failed
irxtkipcvf	ICV failed for TKIP
irxtkipmf	MIC failed for TKIP
irxrf	CCM Replay Failure
irxtkiprf	TKIP Replay Failure
irxdip	Defragmentation in Progress
irxdf	Defragmentation Failure
irxex	Exception - Reserved value
wep40	WEP-40 encrypted

Table 273 GS2000 WLAN RX Statistic Counters (Continued)

WLAN Statistic Counters	Description
wep104	WEP-104 encrypted
tkip	TKIP encrypted
ccmp	CCMP encrypted
unencryp	Not encrypted
ukencryp	Unknown encryption
leg	Legacy
ht20l	HT-LongGl-20MHZ
ht20s	HT-ShrtGl-20MHz
ht40l	HT-LongGl-40MHz
ht40s	HT-ShrtGl-40MHz
mcs32s	MCS-32 ShortGl
mcs32l	MCS-32 LongGl
bcn	Beacon
rts	RTS
cts	CTS
ack	ACK
probersp	Probe response
probereq	Probe request
atim	ATIM
cfend	CF-End
back	Block-Ack
bar	Block-Ack Request
mc_data	Multicast data
uc_data	Unicast data
oth_data	Other data
qos_uc_data	Multicast QoS data
qos_mc_data	Unicast QoS data
qos_oth_data	Other QoS data
amsdu_uc_data	Multicast AMSDU data
amsdu_mc_data	Unicast AMSDU data
amsdu_oth_data	Other AMSDU data
oth_mgmt	Other Management frame
oth_ctrl	Other Control frame
oth	Other type

3.26.10 Hardware Cryptography

This command is used to enable or disable hardware cryptography block. This feature is used when user uses security features such as SSL, WPS, EAP, and so on. Hardware cryptography is enabled by default in Serial to WiFi.



NOTE: If the user wants to save power or does not want to use this feature, then they are allowed to switch off the hardware crypto block. The SW internally keeps a count of ON and OFF requests and when the count becomes 0, it is switched off.

Command Syntax

AT+CRYPTOEN=n

Parameter Description

Table 274, page 302 describes the Hardware cryptography parameters.

Table 274 Hardware Cryptography Parameters

Parameter	Optional/Mandatory	Value	Description
n	Mandatory	1	It enables the hardware crypto block.
		0	It disables the hardware crypto block.

3.27 Over the Air Firmware Upgrade Using External Flash

This set of commands is for firmware upgrade when the external flash is available to download the binaries that are to be upgraded. This module uses the HTTP client to download the binaries from an HTTP server. AT+HTTPCONF command is used to configure any header(s) that need to be present in the HTTP GET request.



NOTE: *Firmware upgrade performed at less than 2.7V is not expected to work as the flash memory in GS modules is designed to start working from 2.7V (minimum).*

3.27.1 FWUP Configuration

This command is used to upgrade firmware via the wireless interface.

Command Syntax `AT+SOTAFWUPCONF=<param>,<value>`

Parameter Description

Table 275, page 303 gives the valid <param> and the description of the respective <value>. <value> is in string format.

Table 275 FWUP Configuration Parameter Values

Parameters	Value
0	Server IP address
1	Server Port
2	Proxy present (0 - Not Present / 1 - Present)
3	Proxy server IP (required only if Param 2 is equal to 1)
4	Proxy server Port (required only if Param 2 is equal to 1)
5	SSL enabled (0 - Not Enabled / 1- Enabled)
6	CA certification name (if it's already been added using the AT+TCERTADD command)
7	GS2000 binary request URL

Table 275 FWUP Configuration Parameter Values

Parameters	Value
9	Server host name
10	GS2000 signature binary request URL
11	Values: 0 or 1 0: Disables domain name check on incoming certificate from server. 1: Enables domain name check on incoming certificate from server. Note: <ul style="list-style-type: none">AT+SSLCONF (See 3.13.13 SSL Configuration, page 199) command should be configured before enabling domain name check using this parameter.AT+LOGLVL (See 3.10.13 Error Code, page 109) command should be configured to select the debug level so that the response of a command will include more information (error reason) in case of an error.When domain name check is enabled and there is an error on domain name mismatch, a warning is displayed as per the configured log level (AT+LOGLVL) and the firmware upgrade terminates.When domain name check is disabled and there is an error on domain name mismatch, a warning is displayed as per the configured log level (AT+LOGLVL) and the firmware upgrade continues.



NOTE: In case of HTTP/S through Proxy, the request URL should be Absolute path and not the relative path.

Command Response This command returns the standard command response to the serial host.

3.27.2 FWUP Start

This command is used to start upgrading the Firmware.

Command Syntax AT+SOTAFWUPSTART=<value>

Usage This command uses the header configured using AT+HTTPCONF command and other required parameters configured using the AT+SOTAFWUPCONF command, starts the http connection, downloads the new images, and starts updating the firmware.

Command Response This command returns the standard command response to the serial host.

Parameter Description

Table 276, page 305 describes the FWUP Start parameters.

Table 276 FWUP Start Parameters

Parameter	Optional/Mandatory	Value	Description
value	Mandatory	3	Upgrade only the App0 and App1 binaries
		4	
		7	
		10	

If the device is operating as a GO, then it stops GO operation.

3.28 ADC Commands

This section contains ADC commands that are applicable for the GS2011M.

Before executing ADC commands, set the GPIOs (20 and 21) by issuing following commands:

- AT+DGPIO=20,1(GPIO 20 is connected to Temperature sensor. ADC channel zero gives temperature.)
- AT+DGPIO=21,1(GPIO 21 is connected to Light sensor. ADC channel one gives luminous intensity value.)



NOTE: ADC commands are only supported with software release 5.1.0 and later.

3.28.1 ADC Configuration

This command is used to configure the ADC.

Command Syntax

AT+ADCCONF=<conf id>,<value>

Parameter Description

Table 277, page 306 describes the ADC Configuration parameters.

Table 277 ADC Configuration Parameters

Parameter	Optional/Mandatory	Value	Description
conf id	Mandatory	1 - mode	The configuration parameter IDs.
		2 - sample frequency	
		3 - threshold select	
		4 - default config	
		5 - Poll read	

Table 277 ADC Configuration Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
value	Mandatory	1 - mode: 0/1/2	When conf id is configured as mode, then one of the following values is used: <ul style="list-style-type: none">• 0 - Continuous read• 1 - Single read• 2 - Periodic read
		2 - sample frequency	When confid is configured as sample frequency, then the value is the frequency at which ADC should sample (example> 100000 is 100KHz).
		3 - threshold select: 0/1/2/3	When confid is configured as threshold select, then one of the following values is used: <ul style="list-style-type: none">0 - No threshold selected1 - Select 0 threshold2 - Select 1 threshold3 - Select 2 thresholds
		4 - default config: 0	When conf id is configured to default configuration, then the value is always 0 which sets default configuration parameters such as: <ul style="list-style-type: none">• Reference voltage - External voltage ref• Power down polarity - ADC power down is high• ADC SUP1P8 Mode Type - sup1p8 2.5/3.3V range• ADC LVL type - Enable• ADC DVDD type - Enabled when external core supply is provided• ADC TRIM type - Disable• ADC start polarity type - Low• ADC clk selection type - XTAL• ADC start cycle - 1• ADC power cycle - 200• ADC FIFO THR - 8 When the value used is other than '0' the following error occurs: ERROR Invalid Input
		5 - Poll read: 0/1	When conf id is configured to Poll read, then one of the following the values is used: <ul style="list-style-type: none">• 0 - Disable single polling• 1 - Enable single polling

3.28.2 ADC Start

This command is used to start the ADC.

Command Syntax AT+ADCSTART

3.28.3 ADC Read

This command is used to read a value using ADC. It should be issued after the Configuration and Start commands.

Command Syntax AT+ADCREAD=<size_of_data>,<channel>

Parameter Description

Table 278, page 308 describes the ADC Read parameters.

Table 278 ADC Read Parameters

Parameter	Optional/Mandatory	Value	Description
size_of_data	Mandatory	1 - 256	This parameter is used to set the number of values to be read from ADC.
channel	Mandatory	0 - 7 Following are the default configuration values: <ul style="list-style-type: none">• 0: Read data from channel zero (Temperature)• 1: Read data from channel one (Light) Channels 2 to 7 are configurable as per user requirements.	This parameter specifies the channel used to read data.

Synchronous Response

Table 279, page 309 describes the synchronous responses and remarks for ADC Read command.

Table 279 ADC Read Synchronous Responses

Responses	Remarks
OK	On successful read this command returns the requested number of data in hex format (prefixed with 0x) and OK.
ERROR	If parameters are not valid.

3.28.4 ADC Stop

This command closes the adapter ADC so no more read operation is performed.

Command Syntax AT+ADCSTOP

Synchronous Response

Table 280, page 310 describes the synchronous responses and remarks for ADC Stop command.

Table 280 ADC Stop Synchronous Responses

Responses	Remarks
OK	Success
ERROR	If parameters are not valid.

3.28.5 Use Case for ADC

Example To read values from channel 0 and channel 1, execute the following commands:

AT+ADCCONF=1, 1

OK

AT+ADCCONF=2, 100000

OK

AT+ADCCONF=4, 0

OK

AT+ADCCONF=3, 0

OK

AT+ADCCONF=5, 1

OK

AT+ADCSTART

OK

AT+ADCREAD=1, 1

OK

AT+ADCREAD=1, 0

OK

3.29 I2C Commands

This section contains I2C specific commands.

3.29.1 I2C Configuration

This command is used to configure the I2C device.

Command Syntax

`AT+I2CCONF=<conf id>,<value>`

Parameter Description

Table 281, page 311 describes the I2C Configuration parameters.

Table 281 I2C Configuration Parameters

Parameter	Conf id	Optional/Mandatory	Value	Description
Master/Slave	1	Mandatory	0 - Slave 1 - Master	Whether the device is Master or Slave.
Slave device address	2	Mandatory	device_add	It is the slave device address which is of 7 bits excluding the lsb. Note: Hex addresses do not use the 0x prefix. For example, If address is 0x10, then only provide 10.
Addressing mode	3	Mandatory	0 - 7 bit mode 1 - 10 bit mode	Whether the slave address is 7 bit or 10 bit.
Clock Rate	4	Mandatory	0 - 100 KHz 1 - 400 KHz Range - 10 KHz to 34000 KHz	It is the clock rate for I2C. Its value is other than 0 and between the range of 10 KHz to 34000 KHz.
Address Mode	5	Mandatory	0 - Current address 1 - Random address	Whether memory access is in current mode or random mode.
SlaveLocAddr	6	Mandatory	Value	It is the address location when random mode is selected.
Memory Address Sel	8	Mandatory	0 - Single byte 1 - Two bytes	Whether Memory Address Sel is single byte for 7 bit mode or two bytes for 10 bit mode.
Source Clock	10	Mandatory	0 - HSRC	It is the source clock for I2C.

Synchronous Response

Table 282, page 312 describes the synchronous responses and remarks for I2C Configuration command.

Table 282 I2C Configuration Synchronous Responses

Responses	Remarks
OK	Success
ERROR INVALID INPUT	If parameters are not valid.

Example

AT+I2CCONF=1,1

This command configures the device as Master.

AT+I2CCONF=2,10

This command configures the device as Slave when Slave device address is 0x20.

3.29.2 I2C Start

This command is used to start I2C device.

Command Syntax

AT+I2CSTART

Synchronous Response

Table 283, page 312 describes the synchronous responses and remarks for I2C Start command.

Table 283 I2C Start Synchronous Responses

Responses	Remarks
OK	Success
ERROR	If device open fails.

3.29.3 I2C Write

This command is used for write operation.

Command Syntax

AT+I2CWRITE=<No. of bytes>,<bytes>

Example

AT+I2CWRITE=4,01020304

The first parameter specifies number of bytes which is 4 and the second parameter specifies the bytes to be written which is 01 02 03 04.

Synchronous Response

Table 284, page 313 describes the synchronous responses and remarks for I2C Write command.

Table 284 I2C Write Synchronous Responses

Responses	Remarks
OK	Success
ERROR	If parameters are not valid.

3.29.4 I2C Read

This command is used for read operation.

Command Syntax AT+I2CREAD=<No. of bytes>

Example AT+I2CREAD=4

The parameter specifies the number of bytes to be read which is 4.

Synchronous Response

Table 285, page 313 describes the synchronous responses and remarks for I2C Read command.

Table 285 I2C Read Synchronous Responses

Responses	Remarks
OK	Success
ERROR	If parameters are not valid.

3.29.5 I2C Stop

This command is used to stop the I2C device.

Command Syntax AT+I2CSTOP

Synchronous Response

Table 286, page 313 describes the synchronous responses and remarks for I2C Stop command.

Table 286 I2C Stop Synchronous Responses

Responses	Remarks
OK	Success
ERROR	If device close fails.

3.30 Pulse Width Modulation (PWM) Commands

3.30.1 PWM Start

This command is used to start the PWM specified.

Command Syntax

```
AT+PWMSTART=<pwm_id>,<start_state>,<polarity>,<period>,<frequency>,<clock_sel>,<prescalar_value>,[<phase_delay01>,<phase_delay12>]
```

In GS 2000 modules, 40 MHz is used as a reference clock by default and the formula for calculating PWM clock is:

$$\text{PWM clock frequency} = \text{Reference clock (40MHz)} / \text{period}$$

Where, the maximum period value is 1000.

This formula is applicable only when *clock_sel* parameter is set to bus clock. The minimum PWM clock frequency generated when *clock_sel* is set to bus clock is 40KHz.

The *prescalar_value* parameter is used along with the PWM clock frequency formula to generate lesser PWM clock frequency as shown below:

$$\text{PWM clock frequency} = \text{Reference clock (40MHz)} / (\text{period} * \text{prescalar_value})$$

Parameter Description

Table 287, page 314 describes the PWM Start parameters.

Table 287 PWM Start Parameters

Parameter	Optional/Mandatory	Value	Description
pwm_id	Mandatory	1: pwm1 2: pwm2 3: pwm3 4: 3 pwm's at a time	PWM identifier.
start_state	Mandatory	0: 0 on state 1: 50% duty cycle	Whether the PWM should start with 0 on state or duty cycle.
polarity	Mandatory	0: normal 1: inverted	It is the polarity of the channel
period	Mandatory	1 to 1000	It is used to calculate the PWM clock frequency. <i>PWM clock frequency formula:</i> PWM clock frequency = Reference clock frequency/period
frequency	Mandatory	0: 40MHz	It is the frequency of the clock selected for PWM.

Table 287 PWM Start Parameters (Continued)

Parameter	Optional/Mandatory	Value	Description
clock_sel	Mandatory	0: Bus clock	The clock should be selected for the PWM. It is either bus clock or output of a prescalar.
		1: Output of prescalar	
prescalar_value	Mandatory	1 to 64	If the <i>clock_sel</i> is 1, then this parameter is used to calculate the PWM clock frequency. <i>PWM clock frequency formula:</i> PWM clock frequency = Reference clock frequency/(period * prescalar_value)
phase_delay01	Mandatory	N/A	It is the delay between the PWM0 and PWM1 pulses if select all PWMs at one time. The value is in the number of PWM clock and should be greater than 0. This parameter is valid, the PWM is selected all (pwm_id is 4).
phase_delay12	Mandatory	N/A	It is the delay between the PWM1 and PWM2 pulses if select all PWMs at one time. The value is in the number of PWM clocks and should be greater than 0. This parameter is valid, the PWM is selected all (pwm_id is 4).

Synchronous Response

Table 288, page 315 describes the synchronous responses and remarks for PWM Start command.

Table 288 PWM Start Synchronous Responses

Responses	Remarks
OK	Success
ERROR	If parameters are not valid.

Example 1

To generate PWM clock frequency of 40KHz, execute the following AT command:

```
AT+PWMSTART=1,1,0,1000,0,1,1,0,0
```

Where,

- `pwm_id = 1`
- `start_state = 1`
- `polarity = 0`
- `period=1000`
- `frequency=0`
- `clock_sel = 1`
- `prescalar_value = 1`
- `phase_delay01 = 0`
- `phase_delay12 = 0`

As per the given values, the formula will be as follows:

$$\text{PWM clock frequency} = 40\text{MHz}/(1000*1)$$

Example 2

To generate PWM clock frequency of 4MHz, execute the following AT command:

```
AT+PWMSTART=1,1,0,10,0,1,1,0,0
```

Example 3

To generate PWM clock frequency of 400KHz, execute the following AT command:

```
AT+PWMSTART=1,1,0,10,0,1,10,0,0
```

Example 4

To generate PWM clock frequency of 100KHz, execute the following AT command:

```
AT+PWMSTART=1,1,0,10,0,1,40,0,0
```

Example 5

To generate PWM clock frequency of 1KHz, execute the following AT command:

```
AT+PWMSTART=1,1,0,1000,0,1,40,0,0
```

3.30.2 PWM Stop

This command is used to stop the PWM that has started using the AT+PWMSTART command.

Command Syntax

AT+PWMSTOP=<pwm_id>

Synchronous Response

[Table 289, page 317](#) describes the synchronous responses and remarks for PWM Stop command.

Table 289 PWM Stop Synchronous Responses

Responses	Remarks
OK	Success
ERROR	If parameters are not valid.

3.30.3 PWM Control

This command is used to change the duty cycle of the pulse generated by PWM.

Command Syntax

AT+PWMCNTRL=<pwm_id>,<duty_cycle>

Parameter Description

[Table 290, page 317](#) describes the PWM Control parameters.

Table 290 PWM Control Parameters

Parameter	Optional/Mandatory	Value	Description
pwm_id	Mandatory	1: pwm1 2: pwm2 3: pwm3 4: 3 pwm's at a time	PWM identifier.
duty_cycle	Mandatory	1 to 99	It is the duty cycle of the pulse.

Synchronous Response

[Table 291, page 317](#) describes the synchronous responses and remarks for PWM Control command.

Table 291 PWM Control Synchronous Responses

Responses	Remarks
OK	Success
ERROR	If parameters are not valid.

Appendix A Data Handling Escape Sequences

This appendix provides the Data Handling Escape Sequences in GS2011M.

The following sections are covered in this appendix:

- [UART Interface, page 319](#)
- [SPI Interface, page 323](#)

A.1 UART Interface

[Table 292, page 319](#) describes the Data Handling using ESC key sequences on the UART interface.

NOTE: Use flow control when data sent is greater than 2048 bytes.

Table 292 Data Handling Using ESC Sequences on UART Interface

Flow Control	Data Mode (Data Type)	Connection Type	Description and Escape <ESC> Command Sequence
SW or HW	Normal (ASCII Text)	TCP client TCP server	<p>This escape sequence selects the specified Connection ID as the current connection. This switches the connection to be used without exiting from the Data mode of operation. Use this sequence to send data from a TCP server, TCP client or UDP client (must be done before data can be received by that client).</p> <p>Module send and receive sequence:</p> <p><ESC>S<CID><data><ESC>E</p> <p>Example: to send user data (e.g., Hello) on CID 1, the format will be:</p> <p><ESC>S1Hello<Esc>E</p>

Table 292 Data Handling Using ESC Sequences on UART Interface (Continued)

Flow Control	Data Mode (Data Type)	Connection Type	Description and Escape <ESC> Command Sequence
SW or HW	Normal (ASCII Text)	UDP client	<p>If UDP client is configured with unicast destination server IP address.</p> <p>Module send and receive sequence:</p> <p><ESC>S<CID><data><ESC>E</p> <p>If UDP client is configured with broadcast destination server IP address (i.e., 255.255.255.255), then:</p> <p>Module expects to receive the following data sequence from Host:</p> <p><ESC>S<CID><data><ESC>E</p> <p>Module sends the following data sequence to Host:</p> <p><ESC>u<CID><IPAddress><space><port><horizontal tab><data><ESC>E</p>
SW or HW	Normal (ASCII Text)	UDP server	<p>This escape sequence is used when sending and receiving UDP data on a UDP server connection. When this command is used, the remote address and remote port is transmitted.</p> <p>Module expects to receive the following data sequence from Host:</p> <p><ESC>u<CID><IPAddress>:<port>:<data><ESC>E</p> <p>Module sends the following data sequence to Host:</p> <p><ESC>u<CID><IPAddress><space><port><horizontal tab><data><ESC>E</p> <p>Example: when Module sends data (e.g., Hello) on CID 0, the format will be:</p> <p><ESC>u0192.168.0.101<space>1001<horizontal tab>Hello<ESC>E</p>

Table 292 Data Handling Using ESC Sequences on UART Interface (Continued)

Flow Control	Data Mode (Data Type)	Connection Type	Description and Escape <ESC> Command Sequence
SW or HW	Normal (Binary)	N/A	Binary data transfer with software or hardware flow control are not supported with ESC sequence.
SW or HW	Bulk (ASCII Text)	TCP client TCP server	<p>To improve data transfer speed, you can use this bulk data transfer. This sequence is used to send and receive data on TCP client, TCP server, or UDP client connection.</p> <p>Module send and receive sequence:</p> <pre><ESC>Z<CID><data length><data></pre> <p>Example: to send a 5 byte user data (e.g., Hello) on CID 1, the format will be:</p> <pre><ESC>Z10005Hello</pre>
SW	Bulk (ASCII Text or Binary)	UDP client	<p>If UDP client is configured with a unicast destination server IP address, then</p> <p>Module send and receive sequence:</p> <pre><ESC>Z<CID><data length><data></pre> <p>If UDP client is configured with a broadcast destination server IP address (i.e., 255.255.255.255), then:</p> <p>Module expects to receive the following data sequence from Host:</p> <pre><ESC>Z<CID><data length><data></pre> <p>Module sends the following data sequence to Host:</p> <pre><ESC>y<CID><IPAddress><space><port><horizontaltab><data length><data></pre>

Table 292 Data Handling Using ESC Sequences on UART Interface (Continued)

Flow Control	Data Mode (Data Type)	Connection Type	Description and Escape <ESC> Command Sequence
SW or HW	Bulk (ASCII Text)	UDP server	<p>This escape sequence is used when sending and receiving UDP bulk data on a UDP server connection. When this command is used, the remote address and remote port is transmitted.</p> <p>Module expects to receive the following data sequence from Host:</p> <pre><ESC>Y<CID><IPAddress:<port>:<data length><data></pre> <p>Module sends the following data sequence to Host:</p> <pre><ESC>y<CID><IPAddress><space><port><horizontal tab><data length><data></pre> <p>Example: when receiving a 5 byte user data (e.g., Hello) on CID 1, the format will be:</p> <pre><ESC>y0192.168.0.101<space>1001<horizontal tab>0005Hello</pre>
HW	Bulk (Binary)	TCP client TCP server UDP client	<p>To improve data transfer speed, one can use this bulk data transfer. This sequence is used to send and receive data on TCP client, TCP server, or UDP client connection.</p> <p>Module send and receive sequence:</p> <pre><ESC>Z<CID><data length><data></pre> <p>Example: to send a 5 byte user data (e.g., Hello) on CID 1, the format will be:</p> <pre><ESC>Z10005Hello</pre>
SW	Bulk (Binary)	N/A	Binary data transfer with software flow control not supported.

A.2 SPI Interface

Table 293, page 323 describes Data Handling using the ESC Sequences on the SPI Interface.

Table 293 Data Handling Using ESC Sequences on the SPI Interface

Data Mode (Data Type)	Connection Type	Description and Escape <ESC> Command Sequence
Normal (ASCII Text)	TCP client TCP server	<ul style="list-style-type: none"> 1. Data transfer is transparent due to byte stuffing at SPI driver level. 2. Byte stuffing must be incorporated in Host controller as per the Adapter guide. <p>Module send and receive sequence:</p> <p><ESC>S<CID><data><ESC>E</p> <p>or Auto mode.</p>
Normal (ASCII Text)	UDP client	<p>If UDP client is configured with an unicast destination server Ip address, then:</p> <p>Module send and receive sequence:</p> <p><ESC>S<CID><data><ESC>E</p> <p>If UDP client is configured with a broadcast destination server IP (i.e., 255.255.255.255), then:</p> <p>Module expects to receive the following data sequence from MCU:</p> <p><ESC>S<CID><data>ESC>E</p> <p>Module sends the following data sequence to MCU:</p> <p><ESC>u<CID><IP Address><space><port><horizontal tab><ESC>E</p>

Table 293 Data Handling Using ESC Sequences on the SPI Interface (Continued)

Data Mode (Data Type)	Connection Type	Description and Escape <ESC> Command Sequence
Normal (ASCII Text)	UDP server	<p>This escape sequence is used when sending and receiving UDP data on a UDP server connection. When this command is used, the remote address and remote port is transmitted.</p> <p>Module expects to receive the following data sequence from Host:</p> <pre><ESC>u<CID><IPAddress>:<port>:<data><ESC>E</pre> <p>Module sends the following data sequence to Host:</p> <pre><ESC>u<CID><IPAddress><space><port><horizontal tab><data><ESC>E</pre> <p>Example: when receiving user data (e.g., Hello) on CID 0, the format will be:</p> <pre><ESC>u0192.168.0.101<space>1001<horizontal tab>Hello<Esc>E</pre>
Normal (Binary)	N/A	Binary data transfer with software flow control is not supported with ESC sequence.
Normal (ASCII Text or Binary)	N/A	Hardware flow control is not supported.
Bulk (ASCII Text or Binary)	TCP client TCP server	<ol style="list-style-type: none"> 1. Data transfer is transparent due to byte stuffing at SPI driver level. 2. Byte stuffing must be incorporated in Host controller as per the Adapter guide. <p>Module send and receive sequence:</p> <pre><ESC>Z<CID><data length><data></pre> <p>Example: to send a 5 byte user data (e.g., Hello) on CID 1, the format will be:</p> <pre><ESC>Z10005Hello</pre>

Table 293 Data Handling Using ESC Sequences on the SPI Interface (Continued)

Data Mode (Data Type)	Connection Type	Description and Escape <ESC> Command Sequence
Bulk (ASCII Text or Binary)	UDP client	<p>If UDP client is configured with a unicast destination server IP address, then:</p> <p>Module sends and receives the following data sequence:</p> <pre><ESC>z<CID><data length><data></pre> <p>If UDP client is configured with a broadcast destination server IP address (i.e., 255.255.255.255), then:</p> <p>Module expects to receive the following data sequence from Host:</p> <pre><ESC>z<CID><data length><data></pre> <p>Module sends the following data sequence to Host:</p> <pre><ESC>y<CID><IP Address><space><port><horizontal tab><data length><data></pre>
Bulk (ASCII Text or Binary)	UDP server	<p>This escape sequence is used when sending and receiving UDP bulk data on a UDP server connection. When this command is used, the remote address and remote port is transmitted.</p> <p>Module receives from Host the following data sequence:</p> <pre><ESC>y<CID><IP Address>:<port>:<data length><data></pre> <p>Module sends the following data sequence to Host:</p> <pre><ESC>y<CID><IP Address><space><port><horizontal tab><data length><data></pre> <p>Example: when receiving a 5 byte user data (e.g., Hello) on CID 1, the format will be:</p> <pre><ESC>y0192.168.0.101<space>1001<horizontal tab>0005Hello</pre>

- This page intentionally left blank -

Appendix B Serial-to-WiFi Commands

This appendix provides a list of supported Serial-to-WiFi Adapter commands.

The following sections are covered in this appendix:

- Command Interface, page 328
- UART/ADAPTER Interface Configuration, page 329
- Profile Management, page 330
- GSLINK, page 331
- CoAP, page 332
- WiFi Interface, page 333
- WiFi Security, page 336
- Wireless Configuration, page 338
- Network Interface, page 339
- Connection Management, page 342
- Battery Check, page 345
- Power Management, page 346
- Auto Connection, page 347
- RF Test, page 348
- ADC Commands, page 349
- I2C Commands, page 349
- PWM Commands, page 350
- Miscellaneous, page 351
- Default Return Messages, page 354
- Escape Sequence Commands, page 355

B.1 Command Interface

Table 294, page 328 lists the Command Interface AT commands.

Table 294 Command Interface AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT	None	“OK”	GS2011M
ATEn	$n=0$ (disable) $n=1$ (enable)	IF 1, echo all input	GS2011M
ATVn	$n=0$ (disable) $n=1$ (enable)	IF 1, responses are ASCII, else numerical codes	GS2011M

B.2 UART/ADAPTER Interface Configuration

Table 295, page 329 lists the UART/ADAPTER Interface AT commands.

Table 295 UART/ADAPTER Interface Configuration AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
ATB	<baudrate>[[,.bitsperchar>]][,<parity>][,<stopbits>]	UART parameters are immediately reset to values provided.	GS2011M
AT&Rn	n=0 (disable) n=1 (enable)	IF 1, hardware flow control is enabled	GS2011M
ATSn	(n=2 to 7,9; p=parameter value)	Not Supported Sets various timeout values: <ul style="list-style-type: none"> • 2= TCP Connection Timeout • 3= Association Retry Count • 4= Nagle Algorithm Wait Time • 5= Scan Time • 6= L4 Retry Period • 7= L4 Retry Count • 9= Maximum number of recv/recvfrom performed on socket • 	GS2011M
ATIn	n=value	Various Adapter ID information: <ul style="list-style-type: none"> • 0=OEM ID • 1=Hardware Version • 2=Software Version 	GS2011M
AT+WST	<Min scan time>,<Max scan time>	Min scan time is the minimum scan time per channel. Max scan time is the maximum scan time per channel. The Max scan time should always be greater than or equal to Min scan time. Both parameters are in milliseconds. This command also modifies the scan time configured with the ATS5 command.	GS2011M

B.3 Profile Management

Table 296, page 330 lists the Profile Management AT commands.

Table 296 Profile Management AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT&Wn (see Note 1)	$n=0$ (profile 0) $n=1$ (profile 1)	Save profile specified by n .	GS2011M
ATZn	$n=0$ (profile 0) $n=1$ (profile 1)	Load profile specified by n .	GS2011M
AT&Yn (see Note 1)	$n=0$ (profile 0) $n=1$ (profile 1)	Set default profile to the value n .	GS2011M
AT&F	None	Restore profile to factory default values.	GS2011M
AT&V	None	Current and saved profile parameter values as ASCII.	GS2011M

Note 1: Only supported for GS1011MGS1500M firmware release 2.4.33.4.3 and earlier. The latest firmware releases for GS1011M (2.5.1)GS1500M (3.5.1) support only one profile. The GS2011MGS2100M supports two profiles.

B.4 GSLINK

Table 297, page 331 lists the GSLINK AT commands.

Table 297 GSLINK AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+WEB SERVER	<0=Stop/1=Start>,<username>,<password>,[1=SSL enable/0=SSL disable],[idle timeout],[Response Timeout]	This command is used to start/stop the web server and register/de-register the default URI (/gainspan/profile/mcu).	GS2011M
AT+XMLPARSE	n:Enable/Disable XML parsing	This command enables/disables xml parsing.	GS2011M
AT+XMLSEND	<CID>,<Type>,<Timeout>,<PageURI>,<Roottagname>[,<N>],<Send response status line>,<Send response headers count><ESC>G<CID><len><tagname>:<value>	XML Data Send	GS2011M
AT+URIRECV	<URI>[,content Type,]	Modify the default adapter URI to the new one.	GS2011M

B.5 CoAP

Table 298, page 332 lists the CoAP AT commands.

Table 298 CoAP AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+CoAPOPTCONF	<Param>,<Value>	Configures the CoAP parameters and values	GS2011M
AT+CoAPOPTCONFDEL	<Param>	Removes CoAP client configuration	GS2011M
AT+CoAPOPEN	<DTLS Flag>	Creates CoAP content and returns CID.	GS2011M
AT+CoAPSENDRECEIVE	<CID>,<coap-uri>,<connection method>,<connection type>,<response Timeout>,[<payload size>,<payload Type>,<payload>]	Opens a CoAP client and connects to the server specified by the host name and IP address.	GS2011M
AT+CoAPCLOSE	<CID>	Closes the CoAP client connection identified by the CID.	GS2011M

B.6 WiFi Interface

Table 299, page 333 lists the WiFi Interface AT commands.

Table 299 WiFi Interface AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+NMAC	<MAC ADDRESS>	Sets the adapter MAC address (an 8-byte colon-delimited hexadecimal number), and stores the value in Flash memory.	GS2011M
AT+NMAC	?	Returns the current adapter MAC address.	GS2011M
AT+WREGDOMAIN	<Regulatory Domain>	<ul style="list-style-type: none"> FCC-supported channel range is 1 to 11. ETSI-supported channel range is 1 to 13. TELEC-supported channel range is 1 to 14. 	GS2011M
AT+WREDOMAIN	?	Outputs the configured regulatory domain in the Serial-to-WiFi adapter.	GS2011M
AT+WS	[<SSID[,<BSSID>][,<Channel>][,<ScanTime>]]	Network scan, returns list of found networks in the format: <SSID>,<BSSID>,<Channel>,<RSSI>,<Mode>,<Security> SSID may be a string of up to 32 ASCII characters in length.	GS2011M
Note: <Scan Time> is not used in GS2000. Use the AT+WST to set the scan time for GS2000.			

Table 299 WiFi Interface AT Supported Commands (Continued)

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+WM	n[,<beacon interval in AP mode>,<broadcast ssid in AP mode>,<no. of stations allowed in AP mode>,<dtim period in AP mode>,<inactivity timeout in AP mode>,<group key renewal interval in AP mode> 0 - station mode 2 - limited AP 5 - ISOTX	Set 802.11 Station operating mode.	GS2011M
AT+WA	<SSID>,[,[<BSSID>],[<Ch>],[Rssi Flag]]	Associate to specified SSID, BSSID, and channel. RSSI is an optional parameter with values: <ul style="list-style-type: none">• 1 - associate to the AP specified by SSID with highest RSSI value.• 0 - associate to the AP specified by SSID without considering RSSI value. This is the default settings.	GS2011M
Note: RSSI Flag is not used in GS2011M. The default behavior is associated with highest RSSI.			
AT+WD	None	Disassociate from the current network.	GS2011M
AT+WWPS	For Push Button (PBC) method: <METHOD>[,PIN][,StoreL2ConnInfo][,SSID] For Pin method and Default Pin method: <METHOD>[,PIN][,SSID][,StoreL2ConInfo]	Associate to an AP using WPS. Upon execution of this command, the GS node uses either push button or pin method or default pin method as per the METHOD parameter to associate to the WPS enabled AP. Store L2connection stores the connection parameter into profile after successful WPS association.	GS2011M
AT+NSTAT	?	Current wireless and network configuration.	GS2011M

Table 299 WiFi Interface AT Supported Commands (Continued)

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+WSTATUS	None	Adapter reports the current network configuration to the serial host	GS2011M
AT+WRSSI	?	Current RSSI as ASCII	GS2011M
AT+WRATE	value<Transmit rate of data frame>[,<Transmit rate of management frame>,<Transmit rate of control frame>]	Sets the transmit rate	GS2011M
AT+WRATE	?	Obtain the current transmit rate (in ASCII format) of the data frame.	GS2011M
AT+APCLIENTINFO	?	Get the information about the clients associated to the adapter when it acts as a limited AP.	GS2011M

B.7 WiFi Security

Table 300, page 336 lists the WiFi Security AT commands.

Table 300 WiFi Security AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+WAUTH	<i>n</i> =1 to 2	Authentication mode setting	GS2011M
AT+WWEP <i>n</i> (see Note 1 below)	<i>n</i> =1 to 4, <key>	WEP key <i>n</i> is set to the value in <key>.	GS2011M
AT+WWPA	<passphrase>	WPA passphrase set to the value in <passphrase>.	GS2011M
AT+WPAPSK	<SSID>,<passphrase>	Computes and stores the WPA2 PSK value.	GS2011M
AT+WPSK	<PSK>	Sets the WPA2 pre-shared key to the <PSK>.	GS2011M
AT+WEAPCONF	<OuterAuthentication>,<Inner Authentication>,<user name>,<password>[,<PE AP with Certificates>]	<p>Sets the Outer authentication, Inner authentication, user name and password for EAP Security. This command returns the normal response codes.</p> <p>The valid outer authentication values are:</p> <ul style="list-style-type: none"> • EAP-FAST:43 • EAP-TLS:13 • EAP-TTLS:21 • EAP-PEAP:25 <p>The valid Inner authentication values are:</p> <ul style="list-style-type: none"> • EAP-MSChAP:26 • EAPGTC:6 <p>For PEAP with Certificates, set the [PEAP with Certificates] field to “1”.</p>	GS2011M

Table 300 WiFi Security AT Supported Commands (Continued)

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+WEAP	<Type>,<Format>,<Size>,<Location><CR><ESC>W<data of size above>	Configures certificate for EAP-TLS	GS2011M
AT+WEAPTIMECHK	• 0 - Disable • 1 - Enable	Enables or disables time validation for EAP certificate. Default value = 1	GS2011M
AT+TCERTADD	<Name>,<Format>,<Size>,<Location><CR><ESC>W<data of size above>	Configures the certificate for SSL/HTTPS and EAP/TLS	GS2011M
AT+TCERTDEL	<certificate name>	Deletes a certificate from memory.	GS2011M
AT+SRVVALIDATIONEN	• 0 - Disable • 1 - Enable	Enables or disables server's certificate validation on DUT. Default value = 1	GS2011M
AT+WSEC	• 0 - Auto security (All) • 1 - Open security • 2 - WEP security • 4 - WPA-PSK security • 8 - WPA2-PSK security • 16 - WPA Enterprise • 32 - WPA2 Enterprise • 64 - WPA2-AES+TKIP security	The S2W adapter supports either one of the values with default security configuration as "Auto." This strict security compliance is not applicable for the WPS feature.	GS2011M

Note 1: The AT+WWEPn command specifies the Key to be used for Key number *n* of the WEP security to connect to an AP. APs can use 1 of 4 WEP keys (key 1 through 4).

For example,

If setting Key 1, the command would be:

AT+WWEP1=<key>

If setting Key 2, the command would be:

AT+WWEP2=<key>

B.8 Wireless Configuration

Table 301, page 338 lists the Wireless Configuration AT commands.

Table 301 Wireless Configuration AT Supported Commands

Command	Parameters	Response/ Effect	GS Module(s) Supported
AT+WRXACTIVE	$n=0$ (disable) $n=1$ (enable)	IF 1, 802.11 radio is enabled.	GS2011M
AT+WIEEEPSPOLL	$<n>[,listen beacon interval][,WakeupType][,Wakeup Interval][,Beacon Wait timeout][,DataRxType][,ActiveToOffTimeout][,SwitchToActivePeriod]$	<p>$n=0$, to disable $n=1$ to enable</p> <p>If it is enabled then the second parameter listen beacon interval is valid beacons intervals at which the WLAN wakes up for listening to the beacon. Although it's a 16-bit value, the maximum recommended is 10-bit value.</p> <p>On execution of this command, the adapter will set the listen interval for n beacons.</p> <p>For GS2011M the listen beacon interval is the listen interval that will be advertised in the association request.</p> <p>The valid values are:</p> <ul style="list-style-type: none"> DTIM-0 LISTEN INTERVAL-1 CUSTOM-2 <p>Wake Up Interval -This is valid only if Wake Up type is Listen Interval and CUSTOM(2).</p>	GS2011M
AT+WRXPS	$n=0$ (disable) $n=1$ (enable)	IF 1, Power Save mode is enabled.	GS2011M
AT+WSYNCINTRL	$<n>$ 1 to 65535	Configure the sync loss interval.	GS2011M

B.9 Network Interface

Table 302, page 339 lists the Network Interface AT commands.

Table 302 Network Interface AT Support Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+NDHCP	n[,<hostname>,<radio mode>,<lease period>,<retry interval>]	Enable or disable DHCP client support for IPV4 parameters.	GS2011M
AT+DHCPSRVR	<Start/Stop[,<Dns Option Disable>,<Gateway Option Disable>]	Prior to start the server, the adapter should be configured with a valid static IP address. Start/Stop: 1 is for starting the server and 0 is for stopping the server. Dns Option Disable: 1 is for disabling and 0 is for enabling with enable as default setting. Gateway Option Disable: 1 is for disabling and 0 is for enabling with enable as default setting.	GS2011M
AT+NSET	<Src Address>,<Net-mask>,<Gateway>	Static network parameters overrides previous values.	GS2011M
AT+DNS	n,<url> n=0 (disable) n=1 (enable)	URL is the DNS name associated to the DNS IP address.	GS2011M
AT+DNSLOOKUP	<URL>,[<Retry count>,<Retry timeout>]	Queries DNS server for address of hostname URL.	GS2011M

Table 302 Network Interface AT Support Commands (Continued)

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+DNSSET	<DNS1 IP>,<DNS2 IP>]	Sets the DNS server addresses to be used.	GS2011M
AT+NIPMULTICASTJOIN	<GroupIP>	Joins the specified multicast group.	GS2011M
AT+NIPMULTICASTLEAVE	<GroupIP>	Leaves the specified multicast group.	GS2011M
AT+STORENWCONN	N/A	Stores network connection parameters prior to transition to Standby.	GS2011M
AT+RESTORENWCONN	N/A	Restores network connection parameters after wake from Standby.	GS2011M
AT+MDNSSTART	N/A	Starts the mDNS module of the adapter.	GS2011M
AT+MDNSHNREG	[<Hostname>],<Domain name>	Registers the host name for the mDNS.	GS2011M
AT+MDNSHNDEREG	<host name>,<Domain name>	De-registers the host name.	GS2011M
AT+MDNSSRVREG	<ServiceInstanceName>,[<ServiceSubType>],<ServiceType>,<Protocol>,<Domain>,<port>,<Default Key=Val,<key 1=val 1>,<key 2=val 2>...	De-registers the mDNC services.	GS2011M
AT+MDNSSRVDEREG	<ServiceInstanceName>,[<ServiceSubType>],<ServiceType>,<Protocol>,<Domain>	De-registers the mDNS services.	GS2011M
AT+MDNSANNOUNCE	None	Announces the mDNS services.	GS2011M

Table 302 Network Interface AT Support Commands (Continued)

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+MDNSSD	[<Service subtype>],<Service type>,<Protocol>,<Domain>	Discovers the mDNC service.	GS2011M
AT+NARPCHACHEEN	Enable: 1 to start the caching Enable: 0 to stop the caching	Caching of the ARP entries (max 8) in its non-volatile memory and available across standby wakeup cycle.	GS2011M
AT+NARPCHACEDEL	None	Deletes the ARP entries from the adapter network stack.	GS2011M
AT+NARP	?	Lists all ARP entries present.	GS2011M
AT+NARPSET	<Ip address>,<Mac address>	Sets the static entry in the ARP table.	GS2011M
AT+NARPDELETE	<Ip address>,<Mac address>	Deletes the static entry in the ARP table.	GS2011M
AT+NARPAUTO	n	Enables or disables updating ARP entries to network stack.	GS2011M
AT+GRATARP	N/A	Sends gratuitous ARP.	GS2011M

B.10 Connection Management

Table 303, page 342 lists the Connection Management AT commands.

Table 303 Connection Management AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+NCTCP	<Dest-Address>,<Port>	Attempts TCP client connection to Destination; CONNECT<CID> if successful.	GS2011M
AT+NCUDP	<Dest-Address>,<Port>[<,Src Port>]	Open UDP client socket to Destination; CONNECT<CID> if successful. The port range 0xBAC0 to 0XBACF may not be used.	GS2011M
AT+NSTCP	<Port>	Start a TCP server on Port; CONNECT<CID> if successful.	GS2011M
AT+NSUDP	<Port>	UDP server on Port; CONNECT<CID> if successful. The port range 0xBAC0 to 0xBACF may not be used.	GS2011M
AT+CID	?	Returns the current CID configuration.	GS2011M
AT+CLOSE	<CID>	Close connection identified by CID.	GS2011M
AT+CLOSEALL	None	Closes all open connections.	GS2011M
AT+NXSETSOCKOPT	<Cid>,<Type>,<Parameter>,<Value>,<Length>	Configures a socket which is identified by a CID.	GS2011M

Table 303 Connection Management AT Supported Commands (Continued)

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+SSLOPEN	<cid>,[<certificate name>,<client certificate name>,<client key name>]	Opens an SSL connection.	GS2011M
AT+SSLCLOSE	<CID>	Closes an SSL connection.	GS2011M
AT+SSLCONF	<enum>,<value>	Configures size of the SSL buffer and specify the number of DNS entries that can be copied into SSL certificate's buffer.	
AT+HTTPCONF	<Param>,<Value>	Configures an HTTP client	GS2011M
AT+HTTPCONFDEL	<Param>	The adapter removes the HTTP configuration specified by the param.	GS2011M
AT+HTTPOPEN	<host>,<Port Number>,[<SSL Flag>,<Certificate Name>,<Proxy>,<Connection Timeout>,<ClientCertificateName>,<ClientKeyName>]	Opens an HTTP client connection. This command opens an HTTP client on the adapter and connects the server specified by the host name or IP address.	GS2011M
AT+HTTPSEND	<cid>,<Type>,<Timeout>,<Page>,[Size of content],<Send response status line>,<Send response headers count>	GET/POST HTTP data on the HTTP client connection.	GS2011M
AT+HTTPCLOSE	<CID>	Closes the HTTP client connection.	GS2011M
AT+UNSOLICITEDTX	<Frame Control>,<Sequence Control>,<Control>,<Rate>,<Power>,<CCA Enable>,<Frame Length>,<Rx_WaitTime>,<DestAddr>,[<RxAddr3>],[<TxAddr4>]		GS2011M

Table 303 Connection Management AT Supported Commands (Continued)

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+UNSOLICITEDRX	<TypeBitmap>,<IEFilterEnable>,<IEID>,<Channel>,<Rx_WaitTime>	<p>Unsolicited data reception.</p> <p>Rate: is the rate at which the data to be received and the possible values are:</p> <ul style="list-style-type: none"> • RATE_1MBPS=130 • RATE_2MBPS=132 • RATE_5_5MBPS=139 • RATE_11MBPS=150 	GS2011M
AT+UNSOLICITEDRXSTOP	N/A	Stops the unsolicited data reception.	GS2011M
AT+ISOBLINK	<Mode>,<gain(power)>,<Number of sub-blanks>,<Number of blinks>,<Blink interval>,<Message length><Tag ID>,[<Bandwidth>,<Payload>,<Frequency>]	This command starts the ISOTX Transmission.	GS2011M
AT+APCONF	Enable: 1 is for limited AP mode and 0 is for station mode, with default value as 0.	NCMAP parameters can be configured using the auto connect.	GS2011M

B.11 Battery Check

Table 304, page 345 lists the Battery Check AT commands.

Table 304 Battery Check AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+BCHKSTRT	<Frequency>	Start checking battery every <Frequency> (≤ 100) packets transmitted.	GS2011M
AT+BATTLVLSET	<Warning Level>,<Warning Freq>,<Standby Level>	Set the battery warning/standby level to enable the adapters internal battery measuring logic.	GS2011M
AT+BCHK	<Batt.chk.freq>	Reset value of battery check frequency.	GS2011M
AT+BCHKSTOP	N/A	Stop checking battery.	GS2011M
AT+BATTVALGET	N/A	Retrieve the most recent battery check value.	GS2011M

B.12 Power Management

Table 305, page 346 lists the Power Management AT commands.

Table 305 Power Management AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+PSDPSLEEP	<timeout>,ALARM1 POL>,<ALARM2 POL>	Enable SoC Deep Sleep power saving mode.	GS2011M
AT+PSSTBY	<x>[,<DelayTime>,<Alarm1pol.>, <Alarm2pol.>]	Requests transition to Standby for x milliseconds.	GS2011M
AT+WAPPSCFG	<Power-Save Configuration>,<Reserved parameter>,<Receiver on-time after Tx>< Power-Save Behavioral Control>	Enables SoC to enter the power saving mode when no actions are pending.	GS2011M

B.13 Auto Connection

Table 306, page 347 lists the Auto Connection AT commands.

Table 306 Auto Connection AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+WAUTO	<mode>,<SSID>,<BSSID>,[channel]	Sets WiFi parameters to be used for Auto Connect.	GS2011M
AT+N AUTO	<Type>,<Protocol>,<Destination IP>,<Destination Port>	Sets network parameters to be used for Auto Connect.	GS2011M
ATCn	n=0 (disable) n=1 (enable)	IF 1, Auto Connect is enabled on next reboot or AT.	GS2011M
ATA	None	Starts Auto Connect, including association.	GS2011M
ATO	None	Returns to a previous Auto Connect sessions; returns an error if no such session exists.	GS2011M
AT+WEBPROV	<user name>,<passwd>[,SSL Enabled,Param StoreOption,idletimeout,nc mautoconnect, format version]	Provisioning through web pages.	GS2011M
AT+WEBPROVSTOP	N/A	Stops the web provisioning.	GS2011M
AT+NURIREDIR	<URL>	Redirects URL support.	GS2011M

B.14 RF Test

Table 307, page 348 lists the RF Test AT commands.

Table 307 RF Test AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+WRTESTSTART	N/A	Start the RF Test mode.	GS2011M
AT+WRFTESTSTOP	N/A	Stop the RF Test mode.	GS2011M
AT+WFRAMETXTEST	<Channel>,<bandWidth>,<numFrames>,<frameLen>,<txRate>,<txPower>,<destAddr>,<bssid>,<htEnable>,<guardInterval>,<greenField>,<preambleType>,<qosEnable>,<ackPolicy>,<scrambler>,<aifsnVal>,<antenna>	Enable the frame transmission with the given configurations.	GS2011M
AT+WRXTEST	<Channel>,<bandWidth>,<rxFrameTypeFilter>,<rxaddrFilter>,<antenna>	Enables the frame reception.	GS2011M
AT+WRXSTOP	N/A	Stops the frame reception and displays the PER stats.	GS2011M
AT+WTX99TEST	<Channel>,<bandWidth>,<numFrames>,<frameLen>,<txRate>,<txPower>,<destAddr>,<bssid>,<guardInterval>,<greenField>,<antenna>,<cca>,<agc>,<contPreambleMode>,<spreader>,<scrambler>,<preamble>,<preambleType>,<phyTestTxRate>,<modeSelect>	Starts TX99 mode with the given configurations.	GS2011M
AT+WTX100TEST	<Channel>,<bandWidth>,<txPower>,<antenna>,<cca>,<agc>,<contPreambleMode>,<spreader>,<scrambler>,<preamble>,<preambleType>,<testPatternType>,<phyTestTxRate>,<modeSelect>	Starts TX100 mode with the given configurations.	GS2011M
AT+WCARWAVTEST	<Channel>,<bandWidth>,<txPower>,<antenna>,<customWavePeriod>	Starts Carrier Wave mode with the given configurations.	GS2011M

B.15 ADC Commands

Table 308, page 349 lists the ADC AT commands.

Table 308 ADC AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+ADCCONF	<conf id>,<value>	This command configured the ADC.	GS2011M
AT+ADCSTART	N/A	This command starts the ADC.	GS2011M
AT+ADCREAD	<size_of_data>,<channel>	This command reads a value using ADC.	GS2011M
AT+ADCSTOP	N/A	This command closes the adapter ADC from operating.	GS2011M

B.16 I2C Commands

Table 309, page 349 lists the I2C AT commands.

Table 309 I2C AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+I2CCONF	<conf id>,<value>	This command configures the I2C device.	GS2011M
AT+I2CSTART	<N/A	This command starts the I2C device.	GS2011M
AT+I2CWRITE	<No. of bytes>,<bytes>	This command is used for Write operation.	GS2011M
AT+I2CREAD	<No. of bytes>	This command is used for Read operation.	GS2011M
AT+I2CSTOP	N/A	This command stops the I2C device.	GS2011M

B.17 PWM Commands

Table 310, page 350 lists the PWM AT commands.

Table 310 PWM AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+PWMSTART	<pwm_id>,<start_state>,<polarity>,<period>,<frequency>,<clock_sel>,<prescalar_value>,[<phase_delay01>,<phase_dealy12>]	This command starts the specified PWM.	GS2011M
AT+PWMSTOP	<pwm_id>	This command stops the PWM that was started.	GS2011M
AT+PWMCNTRL	<pwm_id>,<duty_cycle>	This command changes the duty cycle of the pulse generated by PWM.	GS2011M

B.18 Miscellaneous

Table 312, page 351 lists the Miscellaneous AT commands.

Table 312 Miscellaneous AT Supported Commands

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+SOTAFWUPCONF	<param>,<value>	<ul style="list-style-type: none"> • 0 - Server IP • 1 - Server Port • 2 - Proxy Preset (0 1) • 3 - Server IP if proxy preset=1 • 4 - Server Port if proxy preset=1 • 5 - SSL Enable (0 1) • 6 - CA Cert Name • 7 - WLAN Binary Request URL • 8 - App0 Binary Request URL • 9 - APP1 Binary Request URL • 10 - GS2000 signature binary request URL • 12 - Web image file name 	GS2011M
Note: In case of HTTP/S through Proxy, the request URL should be Absolute path and not the Relative path.			
AT+SOTAFWUPSTART	<value>	<p>Using the header configured using AT++HTTPCONF command, starts the HTTP connection, download the new images and starts updating the firmware.</p> <p>The <value> indicates which of the 3 binaries need to be upgraded:</p> <ul style="list-style-type: none"> • 3 - Only App0 and App1 • 4 - Only WLAN • 7 - All three binaries 	GS2011M
AT+SETTIME	<dd/mm/yyyy> <HH:MM:SS>	Set the adapter system time.	GS2011M

Table 312 Miscellaneous AT Supported Commands (Continued)

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+GETTIME	?	<p>Provides the current system time followed by the standard command response to the serial interface.</p> <p>The time format comes on the serial interface as follows:</p> <p>=<dd/mm/yyyy>,<HH:MM:SS>,System time in milliseconds since epoch (1970).</p>	GS2011M
AT+DGPIO	<GPIO-NO>,<SET/RESET0/1>	Set or reset (high/low) a GPIO pin.	GS2011M
AT+ERRCOUNT	N/A	<p>The error counts include:</p> <ul style="list-style-type: none"> • Watchdog reset counts • Software reset counts • WLAN abort/assert counts 	GS2011M
AT+VER	?	Return the current adapter firmware versions.	GS2011M
AT+VER	??	Gives more details of the S2W version.	GS2011M
AT+PING	<IP>,[[Trails],[<Interval>],[<Len>],[<TOS>],[<TTL>],[PAYLOAD>]]	PING the IP address provided. Trails=0 will ping until <ESC>C is issued.	GS2011M
AT+ASYNCMSGFMT	n • 0 - Disable this feature • 1 - Enable this feature	S2W Adapter supports an enhanced asynchronous notification method.	GS2011M
AT+RESET	None	Resets the adapter.	GS2011M
AT+WLANSTATS	None	Request that the GS2000M sends statistics that it maintains, including Rx, Tx, and encryption errors.	GS2011M
AT+WLANSTATS	None	Request that the GS2000 sends statistics that it maintains. Including TX, RX, and encryption and errors.	GS2011M

Table 312 Miscellaneous AT Supported Commands (Continued)

Command	Parameters	Response / Effect	GS Module(s) Supported
AT+BDATA	<ul style="list-style-type: none"> • 1 - Enable • 0 - Disable 	Enable or disable bulk data.	GS2011M
AT+DROPDATAEN	n <ul style="list-style-type: none"> • 1 - Enable • 0 - Disable 	Enable or disable dropping input data at Serial-to-WiFi level when there is a socket failure or disconnection.	GS2011M
AT+CRYPTOEN	n <ul style="list-style-type: none"> • 1 - Enable • 0 - Disable 	Enable or disable hardware cryptography block.	GS2011M



NOTE: Parameters in [] are optional. Values are expressed as ASCII text unless specified.

B.19 Default Return Messages

Table 313, page 354 lists the Default Return Messages.

Table 313 Default Return Messages

Status	Message (Verbose Enabled)	Message (Verbose Disabled)
Valid Input	OK	0
Invalid Input	ERROR: Invalid Input	2



NOTE: Other commands can return different ERROR messages.

B.20 Escape Sequence Commands

Table 314, page 355 lists the available Escape Sequence commands.

Table 314 Escape Sequence Commands

Escape Sequence	Description	Module(s) Supported
<ESC>S CID	This escape sequence selects the specified Connection ID as the current connection. This switches the connection to be used without exiting from the Data mode of operation. Use this sequence to send data from a UDP client (must be done before data can be received by that client).	GS2011M
Example: <ESC>S10123456789<Esc>E (where 1 is the UDP client CID and 012...9 is the data to be sent)		
<ESC>U CID remote address: remote port:	This escape sequence is used when sending and receiving UDP data on a UDP server connection. The remote address and remote port is transmitted in ASCII text encoding and terminated with a ';' character.	GS2011M
Example: <ESC>U4192.168.1.1:52:<data><Esc>E		
<ESC>u CID <remote address> <remote port>	This escape sequence is used when sending and receiving UDP data on a UDP server connection. The remote address and remote port is transmitted in binary encoding with the MSB transmitted first. The following example shows the header to transmit a UDP packet using binary addressing taking up 9 bytes (d denoting decimal value): <ESC>u4<192d><168d><1d><1d><0d><52d><data><Esc>E	GS2011M
<ESC>E	End-of-Data sequence, indicating end of a transmit frame, and start of transmission. The data received is sent on the network, and the interface returns to Command mode.	GS2011M
<ESC>K<CID><Length> <type><URI>	This is sent once the URL is fetched by the Remote HTTP client.	GS2011M
<ESC>C	This sequence causes transmission of the data received, after which the currently selected connection is closed, and the interface returns to Command Mode. Any buffered data is sent before the connection is closed.	GS2011M
<ESC>xxx	If an unknown character “xxx” is detected after an <ESC> character the <ESC> and the <xxx> characters are ignored.	GS2011M

Table 314 Escape Sequence Commands (Continued)

Escape Sequence	Description	Module(s) Supported
<ESC>Z<CID><DataLen> gth xxxx 4 ascii char><data>	<p>Each escape sequence starts with the ASCII character 27 (0x1B), the equivalent to the ESC key. The contents of <> are a byte or byte stream.</p> <ul style="list-style-type: none"> • CID is connection id (udp, tcp, etc) • Data Length is 4 ASCII character represents decimal value i.e. 1400 byte (0x31 0x34 0x30 0x30). • Data size must match with specified length. Ignore all command or Esc sequence in between data pay load. 	GS2011M
<ESC>Y<CID>remote address:remote port:<DataLen 4 digit ascii><Data>	This escape sequence is used when sending UDP data on a UDP server connection. When this command is used, the remote address and remote port is transmitted in ASCII text encoding and terminated with a “.” character.	GS2011M
Example: <ESC>Y4192.168.1.1:52:<DataLen><data>		
<ESC>y<CID><remote address><DataLen 4 digit ascii><Data>	This escape sequence is used when receiving UDP data on a UDP server connection. When this sequence is used, the remote address and remote port is transmitted in ASCII text encoding and separated by a space () character.	GS2011M
Example: <ESC>y192.168.1.152<DataLen><Data>		



NOTE: The contents of <> are a byte stream, except for <ESC>; literals outside brackets are ASCII.

