GainSpan Corporation - Confidential

Title: Release Notes
Product: GS2011M/GS2100M Firmware
Version: 5.2.1 GA Release
Date: 2016 Jan 19

RELEASE NOTE HISTORY

These notes cover the changes since 5.1.6 GA, 5.2.0 Beta 1, Beta 2, Beta 3, Beta 4 and GA and 5.2.1.1 Beta.

The GS2011M/GS2100M Firmware includes the following versions of GainSpan Software products

Code	Version #	Product Description
WFW	5.2.1.9	802.11 MAC/PHY (WLAN) Firmware
GEPS	5.2.1.7	GainSpan Embedded Platform software
S2W	5.2.1.7	Serial to Wi-Fi

Note:

1. GS flash programming tool and Super Block that comes with the package from SDK builder must be used to program the modules.

Supported features

Network Interfaces
* Wi-Fi Station
    - 802.11b/g/n with 802.11n 1x1 HT20 in 2.4GHz
    - WEP-64 Open/Shared, WEP-128 Open/Shared, WPA (TKIP), WPA2 (AES), WPA2 (AES+TKIP) personal security, WPA-Enterprise, WPA2-Enterprise.
    - EAP Type(s)
        - EAP-TLS
        - EAP-TTLS/MSCHAPv2
        - PEAPv0/EAP-MSCHAPv2
        - PEAPv1/EAP-GTC
        - EAP-FAST
        - EAP-TTLS/PAP
    - Standard Legacy and WMM Power save protocols
    - Advanced Switch-To-Active Power Save protocol
    - DTIM and Custom wakeup Intervals for Power Save protocol
    - AMPDU/AMSDU Rx
    - WMM based QoS
    - Association Keep alive with keep alive period configuration
    - Beacon Miss detection with configurable duration
    - Transmit failure indication with configurable fail count
    - Application Driven Rate Adaptation

- Tx/Rx Statistics
- GS2000 Concurrent Mode AP absent period (NOA) handling

* Wi-Fi Limited AP
  - 802.11b/g/n with 802.11n 1x1 HT20 in 2.4GHz
  - Supports WEP-64 Open, WPA-Personal (TKIP), WPA2-Personal (AES), WPA2 (AES+TKIP) personal security
  - Support for 16STAsin Open and WPA2-Personal security.
  - AMPDU Rx for multiple STAs (up to 16 simultaneous sessions)
  - AMSDU Rx
  - Legacy and WMM Power save protocols with power save buffering for up to 16 STAs
  - AP mode power save (sleep between beacons) with advanced options
  - WMM based QoS
  - L2 forwarding between STAs
  - STA inactivity tracking and disassociation
  - Application driven rate adaptation
  - Vendor specific IE support for management frames
  - Tx/Rx statistics
  - Dynamic SSID hiding in beacons and probe responses

* Wi-Fi Direct (P2P Group Member or Client)
  - P2P Device
    - Device Discovery
    - Provisioning Discovery
  - P2P Group Formation
    - GO Negotiation
    - Provisioning using WPS v2.0 PBC & PIN Methods
  - P2P Client
    - Autonomous P2P Client
    - P2P Client legacy and WMM Power Save

* WLAN STA+AP Concurrent Mode
  - Time Division Multiplexing(TDM) based concurrent mode STA+AP concurrent mode
  - Configurable STA:AP operating periods –20:80 and 30:70 supported
  - Separate globally unique MAC address for each interface
  - Legacy and WMM power save operation for STA interface
  - Active and Passive Scan supported in concurrent mode
  - Supports starting and stopping interfaces in any order
  - Maximizing AP operation time when PS STA dozes off early
  - Absent period announcement (Notice of Absence) to avoid data transfers between GS2000 clients andGS2000 concurrent AP during inactive periods, including time spent in calibration and time for concurrent client beacon sync
  - AP interface supports only open and WPA2-Personal (AES) security.
  - STA interface supports WEP-64 Open/Shared, WEP-128 Open/Shared, WPA(TKIP), WPA2(AES), WPA2(AES+TKIP) personal security, WPA-Enterprise, WPA2-Enterprise.

*Note: “Due to time division multiplexing of STA and AP interfaces during concurrent mode operation; there could be data loss in both interfaces in heavily crowded wireless environments (specifically for STA interface). WPS and other data transfer operations may take longer or fail in heavily crowded wireless environments. “

* Supports following protocols
    - IPv4
    - ARP
    - ICMP
    - UDP
    - TCP
    - DHCP Client
    - DNS Client
    - DHCP Server
    - DNS Server
    - HTTP(S) Client
    - HTTP(S) Server
    - TLS 1.0/1.2 client
    - TLS 1.0 Server
    - mDNS/DNS-SD
    - SNTP Client
    - CoAP Client
    - IGMP (Multicast)
    - DTLS Client

* Supports SSL APIs (TLS v1.0/1.2). The following cipher supported
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_RSA_WITH_RC4_128_SHA
    - TLS_RSA_WITH_RC4_128_MD5
    - TLS_RSA_WITH_AES_256_CBC_SHA

* Support for 4K RSA Server Certificate Signed using SHA256, SHA384, and SHA512 with AES Encryption in TLS.

I/O Drivers

* Supports the drivers for the following I/Os
    - SPI
        + Slave (Max clock speed supported 10Mhz)
        + Master (Max clock speed supported 30Mhz)
    - UART (Max baud rate supported 921.6K)
    - SDIO (Max clock rate 33Mhz)
  - PWM
  - ADC (Sigma delta and SAR)
  - I2C
  - I2S

Power Management
    * Supports Standby in Station Mode
    * Supports DeepSleep in Station Mode

Device Management
    * Over the Air FW Update with Digital Signature Verification

    * Over the Host FW Update with Digital Signature Verification

    * Provisioning
       - Web based Provisioning
       - Verified Provisioning using Concurrent Mode
       - WAC Provisioning (using Apple Authentication IC)
       - WPS 2.0 Enrollee (Station Mode)
       - WPS 2.0 Registrar (AP Mode)
       - Group provisioning (For Android Devices)

Unassociated Mode (Beacon Mode)
   * Transmit frames without association
       - Transmit Data, Management and RTS/CTS control frames
       - Transmit timestamp based on 40MHz clock
       - CCA enable/disable, rate, power, channel, etc
    * Receive frames without association
      - Receive Frame filter
      - IE based filter for beacon, probe request and response frames

WLAN RF Tests
    * Transmit
  Frame transmit with various controls like power, rate, etc
      - TX99, TX100 transmissions
    * Receive
      - Frame receive with channel and MAC address controls
      - Statistics display after receive complete/stop

Misc
    * Energy Measurement Unit. Energy measurement unit/module utilizes 16 bit SigmaDelta-ADC's of GS2000, to accurately measure the electrical parameters such as voltage, current, frequency, Power, Energy & Power factor without the help of an external metering IC

Reference Applications
    * Serial to Wi-Fi
    * TLS – Always on sensor application
    * TLS Low Power – Low power sensor application

Dependency table
---
a. SoC: GS2000 D1
b. Modules: GS2011MxxRev 3.3 or later, GS2100MxxRev 3.2 or later, GS2011MxxS 4.1 or later
c. GS2K_Flashprogram_Plusversion 1.2 or later
d. SDK IDE – IAR version 6.5.50

```
-----------------------------------------------------------------------------
          RELEASE NOTES
-----------------------------------------------------------------------------

Release Notes for each product include sections for version,
enhancements, modifications and bug fixes:


+-------------------------------+
+  WFW                          +
+-------------------------------+

  Release
  -------
    5.2.1.9 – 19-Jan-2016

  New Features (Since 5.1.5)
  ------------
* Improved Rx sensitivity and performance through new calibration scheme
and algorithms (Live Cal). For additional details and recommendations on
use of Live Cal, please see the GS2K_LIVE_CAL_AN_00017 App Note.

* Improved Tx performance through module and channel based Tx Gain
setting.

* Enhanced RTS threshold API to select RTS/CTS for ERP protection instead
of cts-to-self (default).


  New Features (Since 5.1.6)
  ------------
   * Enhanced Rate Adaptation Algorithm
   * Wi-Fi Direct (P2P Group Member or Client)
   * STA+AP Concurrent Mode
   * Dynamic SSID hiding in beacons and probe responses in AP mode

  New Features (Since 5.2.0 Beta 1)
  ------------
   * None


  New Features (Since 5.2.0Beta 2)
  ------------
   * Enhanced RTS threshold API to select RTS/CTS for ERP protection
      instead of cts-to-self (default).
   * Passive scan support.

  New Features (Since 5.2.0 Beta 3)
  ------------
   * Notice Of Absence(NOA) advertisement in Concurrent mode AP beacons
      to prevent concurrent AP clients from sending data during AP
      absence.
   * NOA parsing and handling and deferring data transmission during NOA
      in WLAN client mode.
```

* P2P NOA handling in P2P client mode operation.
* NOA store/restore and handling after standby.
* Transmit confirm for use in important transactions.

New Features (Since 5.2.0 Beta 4)
---
* Noise floor calibration and Rx sensitivity improvements.

New Features (Since 5.2.0 GA)
---
* None

New Features (Since 5.2.1 Beta)
---
* None

Modifications (Since 5.1.5 GA)
---
* Modified STA PS beacon sync sequence to overcome issues with APs that send wrong TSF value in beacon timestamp.
* Improved rate adaptation to improve performance and throughput.
* Removed RTS limit, it can be set to values below 256 to use RTS/CTS.
* Improved Keep-alive scheme in STA mode to avoid disassociations due to inactivity timeout.
* Resolved issues in MSDU lifetime timeout feature.(Since 5.1.6 Beta)
* Updated Tx power table to use optimal Tx power across temperature ranges, channels and rates.(Since 5.1.6 Beta)
* Fine tuned CCA (Since 5.1.6 Beta)
* Tx PVT tuning and optimization (Since 5.1.6 Beta)

Modifications (Since 5.1.6)
---
* Live calibration improvements and optimizations.

Modifications (Since 5.2.0 Beta 1)
---
* None

Modifications (Since 5.2.0 Beta 2)
---
* Enhanced Frame sequence numbering to take care of sequence number reset in concurrent mode interface switch.
* Modified STA PS beacon sync sequence to overcome issues with APs that send wrong TSF value in beacon timestamp.
* Removed RTS limit, it can be set to values below 256 to use RTS/CTS.
* Improved Keep alive scheme in STA mode to avoid disassociations due to inactivity timeout.
* Resolved issues in MSDU lifetime timeout feature and enabled MSDU lifetime timeout feature for concurrent mode.
* Updated Tx power table to use optimal Tx power across temperature ranges, channels and rates.

* Fine tuned CCA.
* Tx PVT tuning and optimization.

Modifications (Since 5.2.0 Beta 3)
---
* Fine-tuned rate adaptation algorithm.
* Enhanced AP power save buffering to move pending frames to power save queue when client switches to power save state without fetching all buffered frames.
* Optimized radio turn off following data transmit after standby wakeup.

Modifications (Since 5.2.0 Beta 4)
---
* Live Cal enhancements and updates.
* Fix for WEP-128 open/shared support in station mode.

Modifications (Since 5.2.0 GA)
---
* Rate adaptation improvements.

Modifications (Since 5.2.1 Beta)
---
* Rate adaptation improvements.
* QoS NULL and PSPOLL frame throttling.
* Workarounds for AP issues of not delivering buffered data on receiving QoS NULL trigger and PSPOLL.
* Fix for sync loss not working after standby wakeup if AP is switched off during standby.
* Fixed an issue that affected Tx performance after standby wakeup.
* Rx DCO Live Cal enhancements and updates.

Limitations
---
* In Limited AP, WEP-64 Shared, WEP 128 Open/Shared does not work
* AMPDU Tx(optional in Wi-Fi Alliance Certification) Not supported
* Block-Ack/AMPDU Rx not supported in concurrent mode.

Known Issues
---
* 6952: In concurrent mode, association in EAP security rarely succeeds when AP interface is brought up before the STA interface.

Bug Fixes (Since 5.1.5 GA)
---
* 5900: Unable to scan AP which is hidden with NETGEAR AP dg834g
* 5859: Key 4 of 4 way handshake is not received by AP
* 4884: WPS2.0 association is failing with Linksys AP's

* 5887: Long Run: L4 connection fails in limited AP TCP/UDP long run in personal security
* 5962: Use_Protection bit is not set in limited AP beacon frames when non ERP STAs are associated to limited AP
* 5864: The issue of command, AT+WP
* 5963: NonERP_Present bit is not set in limited AP beacon frames when non ERP STAs are associated to limited AP
* 5933: More number of WLAN CONNECT ERRORs are seen in AssocDissoc test
* 5983: DUT is not sending DE-authentication to TP Link (TL-WA901ND) AP when AP is powered off.
* 5910: DUT is not able to associate to AP in First attempt after reset with D-Link 601.
* 5928: DUT is not able to Associate with Netgear AP WNDR3800
* 5568: Sometimes DUT sends the trigger frame after about 10 seconds once the TIM bit is set by the AP
* 5137: WPA/WPA2 Personal security association fails sometimes
* 5539: When ieeepspoll is configured (DTIM or Custom or Listen interval) sometime after association radio is switching to high
* 5753: DHCP Process takes 2 to 10 seconds to complete with Cisco1600
* 5980: Timeouts happening at WLAN packet Tx -iTxto
* 5988: Observed AP is de authenticating the DUT when Listen interval wakeup is configured.
* 5966: DUT not able to receive Echo Request packet sent first at 39 mbps and later at 1mbps
* 5981: Throughput in Auto rate not comparable to Fixed rate
* 5172: Ping is failing with Cisco Aironet1200 in Power save mode
* 5570: DUT is not able to Associate with Netgear AP WGR614 v7
* 5907: DUT is not able to receive 'N' rates at the very first attempt
* 5746: Any value of scan time less than 10ms does not take effect
* 5824: DHCP slow with Meraki AP - not lease time issue
* 5999: Broadcast and multicast reception is lower when compared to unicast reception
* 5996: DUT is getting Disassociated after some time (Approx 7 mins.) when leaving Idle in Power save mode with Linksys E1000
* 6001: GS2000 disconnects AP after a while
* 6005: Limited AP doesn't remove clients from its list when inactivity timeout is set to 20 or more
* 6053: Long Run:DUT's radio receiver is completely OFF after some iterations when tried deep sleep with data transfer
* 6073: GS2000 disconnects from AP when there is a glitch in beacon time stamp
* 6104: at+wlanstats shows non zero itxto value with throughput test
* 6146: NonERP_Present bit is set in limited AP frames when association with nonERP STA is not fully completed
* 5152: Client compatibility: L3 connection is not happening with SAMSUNG GALAXY TAB GT-P1010 in channel 14

Bug Fixes (Since 5.1.6 Beta)

* 6209: Node takes 2-3 sec delay in acking TCP data when sent from the tcp server
* 5967: DUT sends data packets with retry bit set.
* 6192: DUT sets the retry bit most of the times while sending broadcast frames
* 6148: WLAN dump when doing channel scan (AT+WS), when there are over 90 APs
* 6029: MAC energy detection threshold setting much higher than IEEE spec
* 6205: Tx Data Rate for RTS packets do not change to adapt to channel
* 6185: App Reset- App wd" is observed while doing ping/flood ping when tried with infinite deep sleep
* 6112: Incorrect duration value in frame header for 2, 5.5, 11 Mbps frames
* 6492: TLS Low power always uses the same MAC layer sequence number (0) for transmitted UDP frames
* 6466: GSNode as LimitedAP wrongly setting TIM bit even though station is not in power save
* 6013: Limited AP buffers data and sets the TIM bit for active client
* 6449: PM bit not being signaled properly in broadcast frames
* 6455: Incremental live cal is not triggered for temperature below -33 degrees
* 6441: Wlan Exception occurs during incremental live cal
* 6452: WLAN Exception is observed if DUT is in deepsleep during incremental live cal
* 6458: Long Run : Getting "APP Reset-Wlan Except" While continuous Assoc/Disassoc and Deep sleep after Association
* 6346: wlan exception when customer was running the standby/wakeup in loop
* 6435: Wlan Exception occurs during first time live cal

Bug Fixes (Since 5.2.0 Beta 2)
---

*5148: During TCP data transmission DUT sends ACK packets with Zero MAC Address resulting in dissociation only with Cisco Aironet 1600 AP.
* 5596: Device sometimes sends zero-addressed ACK frames.
* 5578: Gaps where radio does not ACK or transmits
* 5626: Device is Sending Management and Action Frames at 1 Mbps rate
* 5788: DUT is not able to Connect to Autonomous GO using PIN Method

Bug Fixes (Since 5.2.0 Beta 3)
---

* 6565: GS2000 is not able to form group with another P2P devices (e.g. Nexus)
* 5849: After saving the profile in concurrent mode, on reboot DUT is hung.
* 5854: DUT in WAC mode is beaconing with malformed packets
* 6600: [P2P] : DUT is not able to form Group when Intent Value is lesser then Other Device (Nexus)

* 6604: DUT does not send trigger frame when TIM bit is set against its Assoc ID
* 6607: [P2P] : Group Formation Failure with 3rd party Devices (Nexus/Samsung)
* 6610: [P2P] : Group Formation Failure When both DUTs have Different Listen and Operating Channels.
* 6643: [P2P] : Getting "APP Reset-Wlan Except" While joining as P2P Group with Epson Printer.
* 6566: Provision discovery request is not forwarded to MCU before group form.
* 6571: App stops responding after a while giving boot reason as 5
* 6627: Not able to create group with Panasonic phones, since GS2000 doesn’t support invitation response
* 6532: ARP unable to resolve if the client is Concurrent device Client Interface
* 5770: [P2P] : DUT is advertising Beacon Interval as "3.072 ms" in probe Response
* 6535: Limited AP removes the power save STA after inactivity timeout
* 5772: Limited AP wakes up from power save at next TBTT instead of waking up immediately
* 6551: Association doesn't work when incremental live cal is in progress
* 5790: DUT (GS2000) is not able to join 3rd party Autonomous GO (LG-P970)
* 5792: DUT does not support for Immediate Block Ack when concurrent mode is enabled
* 5802: DTIM count not decrementing in LAP beacon frames after some time
* 6584: [P2P] : Group Formation Failure (GO is not responding with M2 Packet)
* 5827: [P2P]:DUT is sending Action frames on Non Social Channels
* 6586: [P2P] : Group Formation Failure (P2P GO is not sending GO Negotiation Confirmation)
* 6589: [P2P] : Group Formation Failure (P2P Client is not responding with M7 Packet)
* 5866: [P2P]:DUT is not adding WPS IE in Probe Request Frames.
* 6593: at+p2pinvite (invitation frame is violating the spec)
* 6605: [P2P] : DUT is not able to form Group with 3rd party Devices (Nexus/Samsung)
* 5868: APP Reset-Wlan Except occurs after starting the DUT in concurrent mode(STA+AP) and leaving it idle.
* 6233: Module doesn't boot if profile is saved with Wi-Fi direct
* 6750: DUT is not able to Associate (DHCP Failed)
* 6474: DTIM count is not decrementing properly since time stamp mismatch is noticed between limited AP beacon frames
* 5647 at+wm=2 gives "Wlan Exception" when Beacon mode or ISO Tx feature is enabled in binary
* 5840: [P2P]:DUT is sending Action frames on Operating Channels defined in AT Commands
* 5867: [P2P]:DUT is doing Full Channel Scan in Wi-Fi Direct Mode.
* 5891: DUT is not able to associate in WPA2 Security with D-Link DIR 636L AP.
* 6671: [P2P] : DUT is not able to form P2P Group (Not starting Authentication after successful GO Negotiation.)
* 6675: [P2P] : P2P GO (GS2000) is not sending any Deauth Frame when dissolving P2P Group.

* 6260: DUT is not able to associate to AP D-Link 636.
* 6161: Limited AP continue to send frames queued in hardware even if STA informs about PM state
* 5791: [P2P]:Got Mem Dump during P2P Scan.
* 6660: DUT sends trigger frame after ~9sec for TIM bit set against Assoc ID in beacon frame
* 5648: Disabling concurrent mode results in APP Reset-Wlan Except
* 5785: Sequence number is not incrementing when concurrent mode is enabled
* 5786: DUT advertizes Short GI for 20MHz and Rx STBC as supported
* 5808: Beacon frames are having the DTIM count as '0' initially
* 6221: Ping from laptop on AP interface fails in concurrent mode
* 6488: P2P FIND phase is not as per the specification
* 6490: 'AT+P2PSETATTR' is documented but disabled in the code.
* 6617: DUT doesn't receive any packet after sending active null function.
* 6651: WLAN Exception occurred when 'at+wm=0' command is issued in automation.
* 6740: Wlan exception occurred while restoring the network connection.
* 5095: Association is not initiating after WSC procedure with the following APs
* 6771: Malformed management frames
* 5137: WPA/WPA2 Personal security association fails sometimes
* 5569: In concurrent mode configuring second interface first leads to WLAN reset
* 6486: S2W/GEPS shall provide an at command/api to trigger scan
* 5644: DUT is not able to Boot-UP, when default mode is Wi-Fi Direct while building binary.
* 5509: GS2011MIE can't associate with 3Com 8760 AP
* 6531: Deauthentication is not sent by the LAP when we do a fast reboot
* 6537: mDNS response not being sent in Concurrent mode
* 6552: wlan assert if data is received in concurrent LAP interface and client interface is connecting
* 6624: Concurrent mode client interface loses connection with standard AP very frequently
* 6663: Key 4 of the 4 way handshake not received
* 6259: DUT-crashed with at-command "at-command at+wparamset=109,11,1,1,63,2,1,1,1,0,2,19,98" for overnight test
* 6527: In AP Mode, Beacons observed with inconsistent interval when audio data transfer in progress
* 5583: TX99 Test Mode Control Register bug
* 6741: concurrent mode stop result wlan exception
* 6775: Sequence number of the STA's broadcast frame which was forwarded by AP is incorrect
* 5692: Disabling the concurrent mode give WLAN reset

Bug Fixes (Since 5.2.0 Beta 4)

* 6894: Wlan Exception occurs during first time live cal
* 6916: Wakeup from standby results in timeout of packet every time
* 6843: APP Reset-Wlan Excepts are seen in HTTP/HTTPS data transfer tests in non-concurrent mode

* 6865: APP Reset-Wlan Excepts are seen in DUT when concurrent mode is enabled and left the DUT idle
* 6869: STA Interface sends trigger frame but does not receive the buffered data from AP
* 6888: APP SW Reset occurs in limited AP while exchanging TCP-UDP data
* 6845: 4 Wlan Exceptions occurred within 20 hours of assocdissoc long run with limited AP
* 6898: Long Run: 4 WLAN Exceptions seen in 12 hours of Concurrent Mode AssocDissoc Test
* 5136: Issues while doing flood ping between limited AP clients
* 6877: Observed Wlan Exception during OTAFU PUSH Method
* 6018: Long Run: at+wa and scan fails after Disassociation Event when tried standby/deep sleep
* 6907: WLAN EXCEPT during first time live cal
* 6908: DUT doesn't transmit the frame according to the retry count for higher values
* 6833: DUT fails to connect back to the AP in personal security after disconnection
* 6852: Limited AP in concurrent mode always sends beacons with sequence number 0 and no probe response are seen
* 6867: AP Interface does not deliver buffered data when legacy client sends PS Poll
* 6988: TLS Low Power not working after coming out of standby
* 6869: STA Interface sends trigger frame but does not receive the buffered data from AP
* 7009: STA sends null frame with P bit cleared in concurrent mode
* 6904: Limited AP sends more than maximum buffered frames per service period in U-APSD power save
* 6945: wlan exception reset noticed during tcp data transfer long run
* 6862: DUT's Radio goes to Always ON mode when at+wm=2 is executed in Concurrent Mode
* 6969: AP is not removing the client from its list even when client deauthenticates AP
* 7061: AP stops beaconing for 2mins and clients are getting disconnected when timer expiry is initiated on STA mode
* 7091: Data transfer on the STA interface fails in personal security when the AP interface is up
* 7082: WLAN doesn’t give any sort of Tx confirmation indication(success or fail) for the UDP packet
* 7085: WLAN doesn’t give the disconnect callback when AP is switched off and ON very within seconds
* 7086: WLAN doesn’t give the disconnect callback when AP is switched off and ON very within seconds
* 7126: In TLS Low Power ADK, ARP packets not seen on AIR
* 7142: [CONC]: DUT is getting hanged while doing mode switching and scanning on both interfaces in loop
* 7036: Association/data transfer fails in TKIP/WEP security in STA interface of concurrent mode

Bug Fixes (Since 5.2.0 GA)
---
* 7236: TX99 and FRAMETX transmit for 5 seconds and stop

Bug Fixes (Since 5.2.1 Beta)
---
* 6868:HT protection mechanism is not working as expected
* 7264:Module not fetching data buffered in AP for 'n' consecutive beacons
* 7323:AP doesn’t send data to DUT even when the trigger frame has been sent
* 7256:Association request issued with power mgmt flag set to 1
* 7207:No packet sent from the GS limited AP when client moves to lower signal strength
* 7263:Beacon sequence number and time stamp is rolling over intermittently
* 6604:DUT does not send trigger frame when TIM bit is set against its Assoc ID
* 6811:DUT (GS2000) is not able to join Autonomous GO (LG-P970)
* 6956:APdeauthenticates DUT in STA interface since DUT is not able to receive any packets observed when left Idle
* 5767:[P2P] : DUT is not able Scan after After Ping Long Run for 48 hours
* 7265:Enhancement Request: after exceeding maximum association limit in limited AP, allow STA association provided there is an authenticated STA is present in the authenticated/associated STA list
* 7169:Wlan not sending mac level ack success or fail indication for UDP packet
* 7253:DHCP process fails sometimes in STA+AP Concurrent mode for STA interface
* 7286:Initial data rates are not set properly in rate adaptation
* 7296:WLAN Exception is observed when continuous scanning is done for all channel
* 7299:Rate adaptation algorithm is not working if LAP's client is in power save mode
* 7038:Micromax (Model AQ4501) fails to associate with WPS Registrar

```
+-------------------------------+
+  GEPS                         +
+-------------------------------+
```

Release

5.2.1.7 – 12-Jan-2016

New Features (Since 5.1.5 GA)
---
* None

New Features (Since 5.1.6)
---

* Support for Concurrent Mode (STA+AP)
* Support for WAC Provisioning (using Apple Authentication IC)
* Support for Verified Provisioning using Concurrent Mode
* Support for Wi-Fi Direct
  - P2PGroup Member or Client
  - Provision discovery
  - Group formation
  - Persistent group
  - Invitation
* Support for Domain Name Parsing in Incoming Certificate
* Support for sub one second accuracy in SNTP procedure
* Support for timers in GEPS for achieving micro second resolution
* Support for custom HTTP Headers
* Support for CGI arguments in the HTTP URI
* Support for application specific rate adaptation
* Support for Unassociated data transfer in connected mode
* Enhanced DHCP Server to support DHCP Decline
* WPS Registrar support

New Features (Since 5.2.0 Beta 1)
---
* None

New Features (Since 5.2.0 Beta 2)
---
* Domain Name Verification for SSL including HTTPS
* Ability to configure the Retry Interval for DHCP Client
* Ability to configure the Lease Time Requested by DHCP Client
* Ability to configure erase time and verify erase for External Flash FWUP.
* Socket Option to set Max TCP TX Queue depth
* Socket Option to set the TCP Retry Period to less than 1s.

New Features (Since 5.2.0 Beta 3)
---
* Support for Anonymous ID in EAP security
* Support for Certificate CN, OUI validation for EAP-TLS
* Support for run time configuration for MIME in HTTP/GSLink
* Support for confirmation callback mechanism for UDP packet

New Features (Since 5.2.0 Beta 4)
---
* Support for DHCP Procedure to skip the DHCP Discovery in case of known IP and starting from DHCP Request

New Features (Since 5.2.0 GA)
---
* None

New Features (Since 5.2.1Beta)
---
* None

Modifications (Since 5.1.5 GA)
---
* None

Modifications (Since 5.1.6 GA)
---
* None

Modifications (Since 5.2.0 Beta 1)
---
* None

Modifications (Since 5.2.0Beta 2)
---
* Improved EMU power factor accuracy
* Improved SNTP accuracy by considering the round trip delay
* Optimization on the SSL Open (Removing the 1s delay)
* DNS Retry period is now linear

Modifications (Since 5.2.0 Beta 3)
---

* EMU library takes care of the various computation error while load is off or unconnected.

Modifications (Since 5.2.0 Beta 4)
---
* None.

Modifications (Since 5.2.0 GA)
---
* None.

Modifications (Since 5.2.1Beta)
---
* None.

Limitations
---
* ID 5069: Group key renewal is not supported in limited AP mode
* ID 5081: In Long Run, OTA-FWU Push Method Upgrade Procedure is not successful some times. The system continues to work properly after failure of the procedure.

Known Issues
---
* ID 5041: Sometimes L3 fails with Trendnet TEW-652BRP AP
* ID 6864: In concurrent mode, DHCP Server sends a NAK with incorrect IP Address to a Request with a valid IP

Bug Fixes: (Since 5.1.5 GA)
---
* ID 5941: The system hangs if the software reset is triggered when the flash controller is in an intermediate state.
* ID 5923: The NCM does not connect with TP-LINK AP when the AP reboots.
* ID 6055: Mismatch of signed character type
* ID 5165, 5991: With 16 clients connected to Limited AP in WPA-PSK security, during data transfer, observed ARP resolution stops in between data transfer on certain clients even though Limited AP forwards the ARP request packet to the client.
* ID 6009: WPS De authenticating with PocketWiFi AP
* ID 6078: Missing _nx_arp_dynamic_entry_set_with_cb API. Added _nx_arp_resolve_notify_set().use this API to register call back and the resolve ip address for which call back is required. then call nx_arp_dynamic_entry_set() API.
* ID 5909: DNS lookup for a malformed request results in appreset
* ID 6031: The HTTP Response does not include “no cache” headers.
* ID 6101: Webserver(with SSL enabled) terminates the connection abruptly while sending huge data to the client. (Since 5.1.6 Beta)
* ID 6191: The node hang on exiting standby (Since 5.1.6 Beta)

Bug Fixes: (Since 5.1.6 GA)
---
* ID 4984: Limited AP doesn't give IP address to clients when client count exceeds 50. This issue is seen in a test setup which has a complex mix of client devices being connected (iPads, iPods, smartphones, laptops, GS1011/2011 clients). The issue is not seen when using only GS1011/2011 clients.

Bug Fixes: (Since 5.2.0 Beta 1)
---
* 5699: SNTP Time Sync shows incorrect time the second time Time Sync is done.
* 5650: APP SW Reset occurs when DTLSclient(DUT) tries to connect with DTLS server
* 5700: ISOTX Blink Functionality is not working

Bug Fixes: (Since 5.2.0 Beta 2)
---

* ID 5089: DHCP Decline is not sent when Duplicate IP address detected
* ID 5941: The system hangs if the software reset is triggered when the flash controller is in an intermediate state.
* ID 5923: The NCM does not connect with TP-LINK AP when the AP reboots.
* ID 6055: Mismatch of signed character type
* ID 5165, 5991: With 16 clients connected to Limited AP in WPA-PSK security, during data transfer, observed ARP resolution stops in between data transfer on certain clients even though Limited AP forwards the ARP request packet to the client.
* ID 6009: WPS De authenticating with PocketWi-Fi AP
* ID 6078: Missing _nx_arp_dynamic_entry_set_with_cb API. Added _nx_arp_resolve_notify_set().use this API to register call back and the resolve ip address for which call back is required. then call nx_arp_dynamic_entry_set() API.
* ID 5909: DNS lookup for a malformed request results in app reset
* ID 6031: The HTTP Response does not include “no cache” headers.
* ID 6101: Webserver(with SSL enabled) terminates the connection abruptly while sending huge data to the client.
* ID 6191: The node hang on exiting standby

Bug Fixes: (Since 5.2.0 Beta 3)
---

* None

Bug Fixes: (Since 5.2.0 Beta 4)
---

* ID 7042: ADC used by live calibration is not protected

Bug Fixes: (Since 5.2.0 GA)
---

* None

Bug Fixes: (Since 5.2.1 Beta)
---

* ID 7245: 'APP Reset-APP SW Reset' occurs while sending response of raw data from HTTPS server.
* ID 5241: When connecting using WPS (Default PIN method) with Buffalo WZR-HP-AG300H AP, Buffalo WZR-300HP AP and ipTimeN904NS AP with a build where WPS2.0 Strict Compliance is enabled, association procedure is not initiated after WPS procedure.
* ID 5238: In Long Run using WPS Default PIN association procedure fails after some iterations.
* ID 7103: In Long Run APP SW RST's were observed while client trying to connect to the WPS registrar.
* ID 7069: Configured listen interval is not taking into effect when associated through WPS in Concurrent mode
* ID 7164: DNS lookup fails after coming out of standby restoring network connection

* ID 7229: mDNS Response to a PTR query is not correct
* ID 7309: OTAFU fails once the web server is restarted after stopping the web server while the OTAFU is going on
* ID 7163: ERROR response from module for "HTTP 204 No Content response" when module is configured with AT+HTTPCONF=3,close
* ID 5294: GS2000 DHCP server's NAK packet containing Lease Time which is not expected.
* ID 7343: APP Reset in continuous association and disassociation in concurrent mode

```
+-------------------------------+
+  Serial to Wi-Fi Application  +
+-------------------------------+
```

Release

5.2.1.7 – 12-Jan-2016

New Features (Since 5.1.5 GA)
---

* New AT command (AT+DROPDATAEN) to drop data when the error happens during data reception. Once this is enabled, the host needs to ensure that the full data segment is sent and the transaction not terminated in the middle.
* New AT command (AT+CIDCONF) for setting the Nagle Timer on a per socket basis.
* New AT commands to control the Live Cal Operation
  - at+wlcalen=<value>
  - at+wlcalstatus=?
  - at+wlcalerase
* Support for Deepsleep when using SDIO interface
* New options in the SSL Conf to set the TLS Version and the Extensions to be exchanged as part of the SSL negotiations (Since 5.1.6 Beta)

New Features (Since 5.1.6 GA)
---

* Support for Concurrent Mode (STA+AP)
* Support for WAC Provisioning (using Apple Authentication IC)
* Support for Verified Provisioning using Concurrent Mode
* Support for Wi-Fi Direct
  - Autonomous Station (at+p2pjoin)
  - Provision discovery (at+p2ppd)
  - Group formation (at+p2pgrpform)
  - Persistent group
  - Invitation
* Support for initiating OTAFU using Domain Name
* Support for Domain Name Checking in Incoming Certificate. Mismatch reported to the host when the loglvl set to 1 in case of SSL/HTTPS Open on command prompt. Mismatch based action (action specified in the enhanced at command) is taken in case of OTA-FU using HTTPS.
* New AT command (AT+CERTINFOGET) to provide the validity of the provisioned certificate.
* New AT command (ats9) to configure the number of max packets received on a given socket before checking the other sockets (round robin fashion)
* New AT command (at+mdnsstart) to check the status of mDNS (started or stopped)
* New AT command (AT+WEBSERVER) to check if the webserver is started or stopped
* New AT command (AT+HIBERNATE) to support going to the hibernate mode (260nA) mode

* Support for setting the phy mode (b only, g only, b/g only, b/g/n (default), g/n only) in Limited AP using AT+WPHYMODE
* Support for application specific rate adaptation. This can be specified in the at+wm command using the device type and minimum application throughput requirement parameter.
* Support for Unassociated data transfer in connected mode
* New AT command (AT+FWINFOGET) for checking the presence of firmware images for OTAFU
* Support for Client Authentication in the OTAFU using HTTPS.

New Features (Since 5.2.0 Beta 1)
---
* None

New Features (Since 5.2.0 Beta 2)
---
* Support for Over the Host Firmware Update (OTHFU)
* Support for SPI Byte Stuffing as per GS1011
* Domain Name Verification for SSL.
  This is enabled using the command AT+SSLCONF=<Domain name check>, <Buffer size>. For Details refer to Section 3.13.13 S2W Adapter Guide.
* Ability to configure the Retry Interval for DHCP Client. In manual mode, use the command AT+NDHCP=n[,<hostname>,<radio mode>,<lease period>,<retryinterval>]. For details refer to section 3.12.1 S2W Adapter Guide. In NCM auto mode, use AT+NCMAUTOCONF=<Conf Id>,<Value> command with Conf ID 27. Refer to Section 3.22.2 in the S2W Adapter Guide
* Ability to configure the Lease Time Requested by DHCP Client. In manual mode, use the command AT+NDHCP=n[,<hostname>,<radio mode>,<lease period>,<retryinterval>]. For details refer to section 3.12.1 S2W Adapter Guide. In NCM auto mode, use AT+NCMAUTOCONF=<Conf Id>,<Value> command with Conf ID 26. Refer to Section 3.22.2 in the S2W Adapter Guide.
* Updated the AT+WEBPROV command with an optional parameter for the format of the output. If this is set to 1, additional information about the WEP Auth Type is also passed to the host.
* New command AT+GRATARP to send the grat ARP.
* New AT command (AT+DROPDATAEN) to drop data when the error happens during data reception. Once this is enabled, the host needs to ensure that the full data segment is sent and the transaction not terminated in the middle.
* New AT command (AT+CIDCONF) for setting the Nagle Timer on a per socket basis.
* Support for Deepsleep when using SDIO interface
* New options in the SSL Conf to set the TLS Version and the Extensions to be exchanged as part of the SSL negotiations

New Features (Since 5.2.0 Beta 3)
---
* Support for Domain Name instead of IP address in CoAP Open
* New AT command (AT+ARPRESOLVE) to resolve ARP

New Features (Since 5.2.0 Beta 4)

* None

New Features (Since 5.2.0 GA)

* None

New Features (Since 5.2.1Beta)

* None

Modifications (Since 5.1.5 GA)

* The SPI Byte Stuffing is modified to support clock rate up to 2MHz and throughput up to 900Kbps.
* The PMK Cache store increased to 3 (previously 1)
* The GS2000 in auto mode does not send the L3 connect information at the start of the auto mode
* Boot time optimization. The temp reading is done in parallel to the S2W code load.
* The auto mode compatible to GS1011 can be enabled on the builder as the default behavior (Since 5.1.6 Beta)
* The ats8 is now used to set to auto mode frame size (backward compatible with GS1011). The atsa is now used to set the auto mode exit timeout
* The baud rate setting command ATB=<value> is now made backward compatible to GS1011 by default. The default mode can be disabled on the builder.

Modifications (Since 5.1.6 GA)

* Enabled HW auto cache for the GEPS patches
* Optimized the boot time. The temperature read at boot time done in parallel to the S2W code load.
* Timeout of the SysQual for Network Task increased from 32s to 180s
* When the periodic SNTP is requested through AT command, the first SNTP exchange is started immediately and not after the periodic timer expiry
* With NCM, L4 retry period is now set to be infinite by default
* Enhanced auto connection based on GPIO signaling only. Removed the sending of L3 connect information at the start.

Modifications (Since 5.2.0 Beta 1)

* None

Modifications (Since 5.2.0Beta 2)

* Increase the Timeout of the SysQual for Network Task from 30s to 180s
* Default TCP Retry Period changed to 1s (earlier 2s) and number of retries changed to 75 (earlier 12).

* TimeSync first invocation is when the command is issued and then periodically after the time period configured. Earlier, the first invocation was after the first time period expiry
* The SPI Byte Stuffing is modified to support clock rate up to 2MHz and throughput up to 900Kbps.
* The PMK Cache store increased to 3 (previously 1)
* The auto mode compatible to GS1011 can be enabled
* The ats8 is now used to set to auto mode frame size (backward compatible with GS1011). The atsa is now used to set the auto mode exit timeout

Modifications (Since 5.2.0 Beta 3)
---

* To improve throughput, the packet length changed from 1000 to 1460 in case of HTTP Transmit

Modifications (Since 5.2.0 Beta 4)
---
* None

Modifications (Since 5.2.0 GA)
---
* None

Modifications (Since 5.2.1 Beta)
---
* None

Limitation
---
* Loading of Provisioning and OTAFU Web Pages with HTTPS multiple times is not consistent on Chrome, Firefox.
* Number of TCP server sockets to be created is limited to 10.
* Static ARP entry cannot be set when DUT in unassociated state
* Sending more than 1KB data using SSL over TCP may stop sending data after several iterations, only headers would be received. Workaround is to send 1KB or less than 1kb chunks of data.
* OTAFU with SSL enabled need sufficient memory to work.
* Firmware Upgrade is not supported with 2MB 3 Copy on GS2100, GS2011 MIES/MIPS
* In WFD, GS2000 does not respond to invitation request.
* EAP association with Anonymous ID and certificate validation check is not supported through provisioning Apps.
* Firmware upgrade from 5.2.0 Beta-3 to Beta-4 will not work.
* ID 5783: OTAFU PULL works only sometimes when concurrent mode is enabled in crowded environment

Known Issues
---
* ID 7167: Using web app, if Advance Options is not selected in configuring wireless and Network settings page, client verification fails

and hence verified provisioning reports failure in web app. Workaround is to select Advance Options check box.

Bug Fixes (Since 5.1.5 GA)
---
* ID 6064: Mdns execute API hangs which results in App Reset because of sys qual
* ID 5932: Limited AP gives default IP range to clients when it is created through 'at+wa' command after stopping NCM auto start in default limited AP mode.
* ID 5997: Disabling NCM and switching between station to AP results in "APP Reset-APP SW Reset"
* ID 6082: Log level is enabled by default in DNS verification
* ID 5987: Crypto is getting enabled after coming out of deepsleep though it is disabled
* ID 5929: 2 OK are observed as command response for atb and at&Rn command.
* ID 5969: Not able to delete custom HTTP client headers
* ID 6111: Default Retransmission timer of TCP is not getting reflected to SSL server
* ID 6171: In roaming case, DUT associates to AP in channel 1 even when other AP having better RSSI exists in other channels
* ID 6041: Junk characters are getting printed on Teraterm while doing DNS check
* ID 6084: Reg domain value is not taking into effect for group provisioning, configured during SDK build.
* ID 6206: Adjusting DHCP lease time after alarm wake up not done properly.
* ID 5382: SPI byte-stuffing is not supported in current release.

Below bugs fixed since 5.1.6 Beta:
---
* ID 6388: Data get corrupt when sent with more than two/three "0x00 " characters using by SPI byte stuffing
* ID 6279: WEP auth parameter is incorrect in Provisioning info sent to the host
* ID 6280: DUT's Radio receiver is getting completely OFF after issuing at+psstby and at+wm=0 commands
* ID 6248:Firmware upgrade from 5.1.6 firmware to 5.1.6 firmware does not work. However firmware upgrade from 5.1.5 GA to 5.1.6 Beta works.
* ID 5797:If the length of <Status Code><':'><Response Phrase> is <=8, then the format in which the client receives the status code is incorrect.
* ID 6248:DUT is hung while doing HTTP PULL Method
* ID 5798:The end of Http headers list is not indicated by any reserved length value on the host.
* ID 6279 - WEP auth parameter is incorrect in Provisioning info sent to the host.
* ID 6415 - "Service Discovery Failed" message is not coming when async message format is enabled on DUT.

* ID 6461 - Registration Success and Registration Failed Asynchronous messages doesn’t start with '\r\n'
* ID 6421 - DHCP server is stopped when 'at+wd' is issued which breaks the back ward compatibility with GS1011
* ID 6423 - 'at+dhcpsrvr' command returns 'ERROR' and 'ERROR INVALID INPUT' for invalid parameters.
* ID 6529 - Socket failure message is printed issuing at+cid when no CID's are present in case of NCM
* ID 6557 - mDNS command response is not backward compatibility with GS1011
* ID 6518 - Build time default host name for mDNS is not taking into effect when limited AP is created through NCM
* ID 6450 - AT+NSTAT reports inconsistent WSTATE value when NCMAUTO is enabled and provided wrong passphrase for WPA/WPA2/WEP security.
* ID 6769: ATB=<value> at command in upper case is not working. Workaround is to use lower case command. (Since 5.1.6 GA released on 17-Aug)

Bug Fixes (Since 5.2.0 Beta 1)
---
* ID 5696: Firmware built with custom web pages were not built correctly in SDK builder.

Bug Fixes (Since 5.2.0 Beta 2)
---
* ID 5696: Firmware built with custom web pages were not built correctly in SDK builder.
* ID 6064: Mdns execute API hangs which results in App Reset because of sys qual
* ID 5932: Limited AP gives default IP range to clients when it is created through 'at+wa' command after stopping NCM auto start in default limited AP mode.
* ID 5997: Disabling NCM and switching between station to AP results in "APP Reset-APP SW Reset"
* ID 6082: Log level is enabled by default in DNS verification
* ID 5987: Crypto is getting enabled after coming out of deepsleep though it is disabled
* ID 5929: 2 OK are observed as command response for atb and at&Rn command.
* ID 5969: Not able to delete custom HTTP client headers
* ID 6111: Default Retransmission timer of TCP is not getting reflected to SSL server
* ID 6171: In roaming case, DUT associates to AP in channel 1 even when other AP having better RSSI exists in other channels
* ID 6041: Junk characters are getting printed on Teraterm while doing DNS check
* ID 6084: Reg domain value is not taking into effect for group provisioning, configured during SDK build.
* ID 6206: Adjusting DHCP lease time after alarm wake up not done properly.
* ID 5382: SPI byte-stuffing is not supported in current release.

* ID 6388: Data get corrupt when sent with more than two/three "0x00 " characters using by SPI byte stuffing
* ID 6279: WEP auth parameter is incorrect in Provisioning info sent to the host
* ID 6280: DUT's Radio receiver is getting completely OFF after issuing at+psstby and at+wm=0 commands
* ID 5797:If the length of <Status Code><’:’><Response Phrase> is <=8, then the format in which the client receives the status code is incorrect.
* ID 6248:DUT is hung while doing HTTP PULL Method
* ID 5798:The end of Http headers list is not indicated by any reserved length value on the host.
* ID 6279 - WEP auth parameter is incorrect in Provisioning info sent to the host.
* ID 6415 - "Service Discovery Failed" message is not coming when async message format is enabled on DUT.
* ID 6461 - Registration Success and Registration Failed Asynchronous messages doesn’t start with '\r\n'
* ID 6421 - DHCP server is stopped when 'at+wd' is issued which breaks the back ward compatibility with GS1011
* ID 6423 - 'at+dhcpsrvr' command returns 'ERROR' and 'ERROR INVALID INPUT' for invalid parameters.
* ID 6529 - Socket failure message is printed issuing at+cid when no CID's are present in case of NCM
* ID 6557 - mDNS command response is not backward compatibility with GS1011
* ID 6518 - Build time default host name for mDNS is not taking into effect when limited AP is created through NCM
* ID 6450 - AT+NSTAT reports inconsistent WSTATE value when NCMAUTO is enabled and provided wrong passphrase for WPA/WPA2/WEP security.

Bug Fixes (Since 5.2.0 Beta 3)
---

* OTAFU from 5.1.6 to 5.2.0 is not working
* ID 6564: For P2P Find, not more than 18 devices can be sent to the host. Workaround is to Stop Find and Start Find after 18 devices have been sent to the MCU.
* ID 6676: GS2000 as GO does not support more than one client.
* Few asynchronous messages does not follow enhanced asynchronous format.

Bug Fixes (Since 5.2.0 Beta 4)
---
* Verified Provisioning is sending credentials to the MCU even in case of failure during verification leading to multiple credentials being sent to the MCU.
* ID 6873: In long run, Digital signature verification failure during OTH firmware upgrade.
* ID 6887: In long runs after several iterations, DUT is hang sometimes when factory image is restored after successful firmware upgrade (OTAFU).
* ID 6903: In long run after several iterations, APP Reset-APP SW Reset occurs when HTTPS client tries to open connection with webserver whose certs are of 4k.

Bug Fixes (Since 5.2.0 GA)
---
* None

Bug Fixes: (Since 5.2.1 Beta)
---
* ID 7341: Observed APP Reset when NCM stop is issued and NCM L4 retries fail.
* ID 6849: In GSLink, APP SW RST's were observed when the packet send without the network interface open.
* ID 7071: Verification is failing during WAC provisioning to WPA2 & WPA/WPA2 personal securities.
* ID 6936: 'APP Reset-APP SW Reset' occurs when Clients connect to DUT in WAC mode
* ID 5448: Disassociation Event based on Tx failure count is not working
* ID 7301: Malloc failure check missing in HTTP Send.
* ID 5051: Upon Layer 3(DHCP renew) failure GPIO19 will not go low in auto connection
* ID 6860: In Concurrent Provisioning, Limited AP's SSID is getting updated in ACTIVE CLIENT PROFILE
* ID 6557: mDNS command response is not backward compatibility with GS1011 in unconnected state
* ID 7293: Connection timeout is not honored for HTTP Send when the SSL is not enabled in the build
* ID 7136: In case when the user stops the AP with WPS Registrar when WPS was in progress, switches to STA mode and switches back to AP with WPS Registrar, WPS Procedure does not start.
* ID 7212: Bidirectional data (both TCP & UDP) transfer with small payload result in system hang
* ID 7201: DUT hangs after sending SYN packet with spoofed source ip address

---

GainSpan Corporation
3590 N. First Street
Suite 300
San Jose, CA 95134
Tel: +1 (408) 627-6500
Info@GainSpan.com