Texas Instruments Incorporated

CC3100\CC3200 Networking Rev-1 SP PKG 1.05

Release Notes

Released - August 31, 2016

Table of Contents

1 General Information

This document describes the Service Pack software release for the CC3100 and CC3200 chipset.
This release was tested with MSP430F5529 Host platforms, CC3200 and Simple Link Studio using CC3100\CC3200 ES1.33 Production device.

The information in this document is targeted to cover the main features and capabilities set provided in production device and the service pack SW, specifically:

- General Information
- Features
- Limitations/Constraints
- Errata

1.1 Product components:

Component	Details
Reference Host Platform	MSP430F5529, SimpleLink Studio for Windows, CC3200 M4 Host
Chip HW Version	CC3100R ES1.33 production device - 3100 0x4000000 CC3200R ES1.33 production device - 3200 0x4000010
HW platform	Booster Pack Rev 4.1, Launchpad Rev 4.1
Host Version	1.0.1.8
Build Version	2.7.0.0.1.4.1.1.1.0.3.34– Service Pack

1.2 SW Package Content

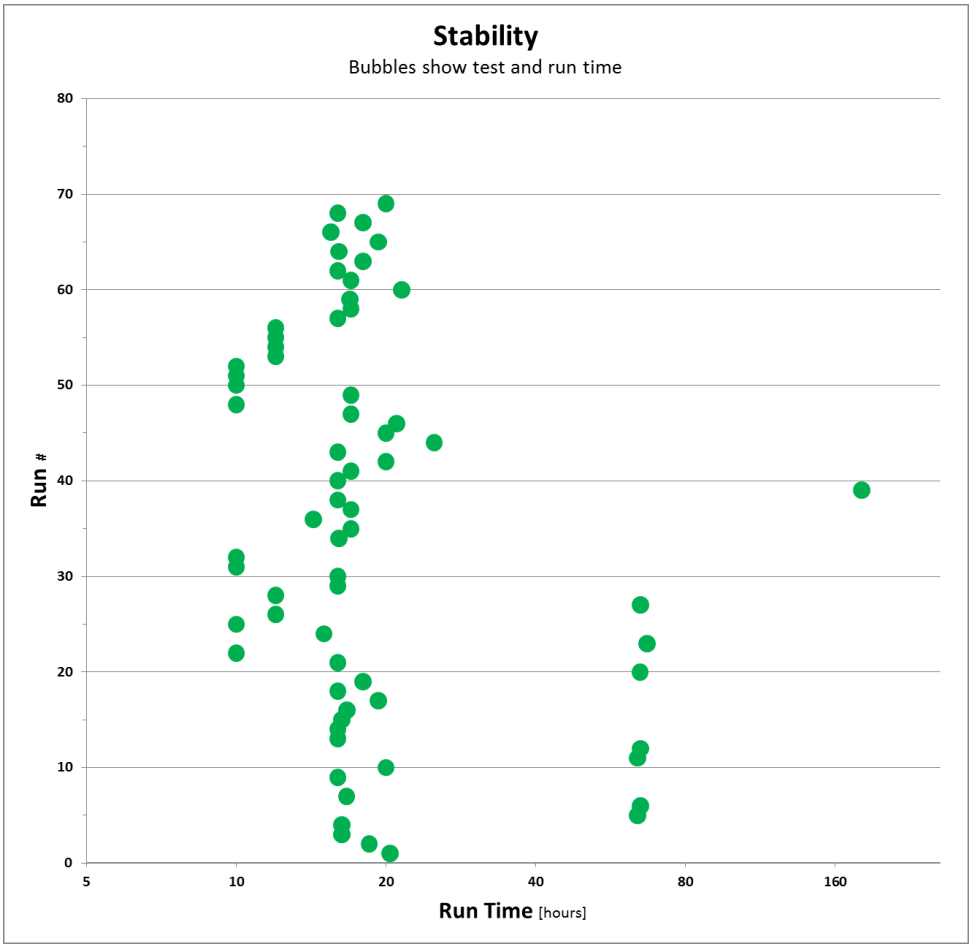
- Host Driver
- Developer Library
  - SimpleLink Studio (for Visual Studio)
  - MSP430
- Binary for the Uniflash Programmer utility encapsulating the SP images
- Signed binary image for OTA

1.3 Package Quality

- Interoperability - IOP
  - STA mode was tested for connection, traffic and power consumption with more than 200 AP
  - AP mode was tested for connection and traffic with more than 50 STA
- Robustness
  - Use cases were tests for 1000 of cycles – for example:
    - Connect/Disconnect
    - On/Off

- Connect, Send Packet, Disconnect

- Stability
  - STA was kept running different traffic scenarios in open AIR for long duration
  - Green Dot - STA was stopped after a set time



2 Features

2.1 Release Highlights

This SW package is a service pack (miscellaneous bug fixes and improvements) for CC3x00 product devices.

2.1.1 Main changes from Package Version 1.0.1.6 SP 2.6.0.5.1.4.0.1.1.0.3.34

- Improved DNS robustness, specifically with large RTT durations (higher than 600mSec)

2.1.1.1 Bug Fixes

Bug fixes - detailed are listed in paragraph 3.4

2.2 Features List

2.2.1 WiFi

Standards	802.11b/g/n **Station** and Wi-Fi Direct **Client**
Supported Channels	1-13 The default regulatory domain is US (1-11)
Personal Security	WEP, WPA and WPA2
Enterprise Security	WPA-2 Enterprise EAP Fast, EAP PEAPv0 MSCHAPv2, EAP PEAPv0 TLS, EAP PEAPv1 TLS, EAP TLS, EAP TTLS TLS, EAP TTLS MSCHAPv2
Provisioning	SmartConfig™ technology Wi-Fi Protected Setup (WPS2) Access Point mode with internal HTTP Web Server

Standards	802.11b/g **Access Point** and Wi-Fi Direct **Group Owner**
Clients	1
Personal Security	WEP, WPA and WPA2

2.2.2 Networking

IP	IPv4
Transport	UDP TCP RAW ICMP
Cross-Layer	DHCP ARP DNS
Application	mDNS DNS-SD HTTP 1.0 web server
Transport Layer Security	SSLV3 SSL_RSA_WITH_RC4_128_SHA SSLV3 SSL_RSA_WITH_RC4_128_MD5 TLSV1 TLS_RSA_WITH_RC4_128_SHA TLSV1 TLS_RSA_WITH_RC4_128_MD5 TLSV1 TLS_RSA_WITH_AES_256_CBC_SHA TLSV1 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLSV1 TLS_ECDHE_RSA_WITH_RC4_128_SHA TLSV1 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

	TLSV1_1 TLS_RSA_WITH_RC4_128_SHA TLSV1_1 TLS_RSA_WITH_RC4_128_MD5 TLSV1_1 TLS_RSA_WITH_AES_256_CBC_SHA TLSV1_1 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLSV1_1 TLS_ECDHE_RSA_WITH_RC4_128_SHA TLSV1_1 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLSV1_2 TLS_RSA_WITH_RC4_128_SHA TLSV1_2 TLS_RSA_WITH_RC4_128_MD5 TLSV1_2 TLS_RSA_WITH_AES_256_CBC_SHA TLSV1_2 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLSV1_2 TLS_ECDHE_RSA_WITH_RC4_128_SHA TLSV1_2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS1_2_TLS_RSA_WITH_AES_128_CBC_SHA256* TLS1_2_TLS _RSA_WITH_AES_256_CBC_SHA256* TLS1_2_TLS _ECDHE_RSA_WITH_AES_128_CBC_SHA256* TLS1_2_TLS _ECDHE_ECDSA_WITH_AES_128_CBC_SHA256* *client
User application sockets	Up to 8 open sockets Up to 2 secured application sockets: - One server (listen socket and accept socket) + client (data socket) - Up to two clients (data socket)

2.2.3 Advanced Features

802.11 Transceiver	Transmit and Receive raw Wi-Fi packets with full control over payload. Wi-Fi disconnect mode. Can be used for general-purpose applications (e.g. tags, sniffer, RF tests)
Traffic Filters	Embedded filters to reduce power consumption and Wake-on-LAN trigger packets (IP and MAC layer)

2.2.4 Interfaces

SPI	Standard SPI up to 20MHz on production device
UART	4 wire UART up to 3MHz

2.2.5 Power Modes

Low Power mode	Uses 802.11 Power Save and Device Deep Sleep Power with three user configurable policies
Configurable Power	• Normal (Default) - Best tradeoff between traffic delivery time and power performance

Policies	• Low power –Used only for Transceiver mode application (Disconnect mode) • Long Sleep Interval – wakes up for the next DTIM after a configurable sleep interval, up to 2 seconds. This policy is only applicable for client socket mode

3 Details

3.1 System/Software Capabilities

- Host SPI interface max speed: 20MHz (production device)
- Stability in all traffic scenarios was tested for at least 12 hours (major use cases were tested for at least 24hours) – User may rarely experience:
  - Traffic Stops
  - System freeze
- Robustness tests
  - Start/Stop with WiFi Connect/Disconnect and data Tx burst was tested for 5000 cycles and found to be stable
  - WiFi Connect/Disconnect without data was tested for 5000 cycles and found stable
- SSL
  - Elliptic-curve based ciphers (e.g. ECDH) implies a longer connection time
- Network Stack
  - TCP Window size: 32KB (Production device)
  - The memory resources are divided among all user sockets and the TCP windows size might change accordingly
  - IP Fragmentation is not supported for Tx UDP and RAW sockets
  - In connection mode Tx and Rx traffic should be done after IP is acquired
- File System
  - Up to 100 user files
- File Size is limited to ~1Mbyte [1,040,384byte] (No Error if trying to create a larger size)
- SPI Interface
  - Little/Big Endian Hosts are supported
  - 8/16/32bit modes are supported
  - Big Endian auto detection is supported
- UART Interface
  - Little Endian Hosts are supported
- HTTP Server
  - Support HTTP 1.0
  - Built-in ROM WEB Pages
  - Additional WEB pages can be stored on the File System
  - Dynamic content through proprietary Token mechanism (limited to 64 Characters)
- WEP
  - WEP open using ASCII pre shared key
  - Small code can be used in the Host and HTTP Web page to support HEX format (more details and code example included in the programmer's guide)
- WPS
  - Delay of up to 4Sec can be seen between association and EAPOL-Start when using WPS connection
- Default State - With no other configuration the default state of the device is as follows:
  - STA mode
  - Regulatory domain is US (channel 1-11)
  - Connection policy – AutoStart and AutoSmartConfig
  - DHCP - Enable

3.2 Product Constraints

- SSL
  - Supported modes
    - Up to one Server (Listen Socket and Accept Socket) + Client (Data socket)
    - Up to Two clients (Data socket)
  - CA Certificates must be installed if server authentication is required
  - Client mode –
    - Signature authentication check – must be less or equal to 2048
    - Key exchange and challenge – must be less or equal to 2048
    - Client authentication – must be less or equal to 2048
  - Server mode –
    - Signature authentication check – must be less or equal to 2048
    - Key exchange and challenge – must be less or equal to 2048
    - Client authentication – must be less or equal to 2048
  - Packets will be truncated above 1386Bytes (two TCP packets will be transmitted)

- SmartConfig
  - Not supported with 5GHz AP (802.11a/n/ac)
  - Not supported for MIMO-capable configuration devices
  - Not supported with non-standard proprietary modulation schemes
  - Only Group 0 is supported in auto start mode
  - In Auto Start Mode the key is transferred not encrypted

- Enterprise Security
  - WPA2-TLS connection is not supported with v3 certificates
  - Connection is successful with expired date certificates

- Tx Power
  - Tx power in AP mode takes effect only after reset

- WiFi Direct
  - When the WiFi Direct is set to be Group Owner (GO) the recommendation will be to set FAST connection policy to TRUE

- Rx Filters
  - BSSID can't be filtered while STA is connected (If filtered will cause disconnection)

- Power Management
  - The device will remain in active after init until the host will read all events

- HTTP internal WEB Pages – main limitations
  - Values entered are not validated – for example:
    - Adding longer/short key in password fields (will be accepted)
    - Typing letters in DHCP lease time (instead of numbers)

  - WPA password is requested to be entered in Hex format when it should be ASCII
  - The length of the AP SSID field is limited to 15 characters (instead of 32)
  - The length of the AP Password field is limited to 24 characters (instead 63)
  - The length of the Device name is limited to 15 characters (instead of 32)
  - Adding/configuring Hidden SSID is not supported
  - HTTP authentication (user name and password) should be disabled in order not to get into a lock state

- Network Stack
  - Max Tx payload for Raw packet with IP header is 1460 bytes
  - Max Tx payload for Raw Transceiver (disconnect mode) is 1476 bytes (including Data and Header)
  - Min Tx payload for Raw Transceiver (disconnect mode) is 14 bytes (including Data and Header)
  - Closing socket should be done in a proper way (for example not to close a socket while there is blocking receive command on it) - a timeout can be used in this scenarios
  - TCP socket keep alive timeout is set to 5Min (non configurable)
- Host
  - The Host driver is assuming that a Char value is equal to 1 Byte. MCU (like CC2000) that support different configuration won't work with the Host Driver as is. The only option is to port the driver manually to the MCU architecture

- Setting device Mode
  - Changing the device role (STA<->AP<->P2P) requires to reset the device
  - Setting network configurations after setting the device role (without reset) can lead to system halt
  - If SetRole to station was issued during AP mode it won't accept connected STA (See first bolt, reset is required)
  - Setting the device mode is persistent and SFLASH endurance must be considered on use cases that requires switching between roles
  - Network configuration is applicable to the current role of the device

- Supported SFLASH

  The product supports JEDEC specification (to read manufacture ID by JEDEC standard) – the below list are the main SFLASH that were verified.
  - Micron N25Q128- A13BSE40 - 128Mbit
  - Spansion S25FL208K - 8Mbit
  - Winbond W25Q16V - 16Mbit
  - Adesto AT25DF081A - 8Mbit
  - Macronix MX25L12835F-M2 - 128Mbit
  - Macronix MX25R6435 – 64Mbit
  - ISSI IS25LQ016 - 16Mbit

  Updated list and more recommendation can be found in: CC3100 & CC3200 Serial Flash Guide

3.3 Performance

Item	Production
Maximum SPI clock speed	20 MHz
Init time from hibernate until device ready	75 mSec
Init time from hibernate until WPA2 connection	120 mSec
Maximum UDP throughput, open socket	16 Mbps
Maximum TCP throughput, open socket	13 Mbps
Maximum TLS/SSL throughput with RC4_128 cipher	9 Mbps
Maximum TLS/SSL throughput with AES_256 cipher	12 Mbps
Minimum TLS/SLL connection time with ECC cipher	1.3 Sec
Minimum TLS/SSL connection time with RSA cipher	130 mSec

3.4 Fixed Items in this release from package Version 1.0.1.6 SP 2.6.0.5.1.4.0.1.1.0.3.34

ID	MCS00135767
Title	Command sl_WlanSet is not working on Big Endian systems
Description	The command is not working well on Big Endian systems and will return an documented error. The command is used to set Tx power, Scan parameters, regulatory domain

ID	MCS00131563
Title	Host: Set/Get time is limited up to year 2038
Description	time.h (standard time library) is limiting the structure to a signed 32-bit integer, and this number is interpreted as the number of seconds since 00:00:00 UTC on 1 January 1970

ID	MCS00135764
Title	SFLASH driver not returning the right status
Description	File system read function might return partial data due to wrong status return from the SFLASH driver

ID	MCS00135857
Title	Fail to open transceiver socket while profile exists
Description	In case of opening a of transceiver socket with ‘auto connection’ policy to set to true and profiles stored, the socket creation might fail.

ID	MCS00136091
Title	IOP : The SimpleLink device fails to associate to a P2P GO in negotiation mode
Description	IOP: In some cases the device will fail to connect to a P2P go device due to shorter timeout in the remote peer device.

ID	MCS00135918
Title	Get scan policy does not return wrong value
Description	Get scan policy does not return the correct value - if device was started and scan policy was never enabled, the get API will return 1 instead of 0.

ID	MCS00136131
Title	DNS Request failure on RTT larger than 600mSec
Description	When the DNS client is waiting for specific transaction ID and the response will be received after the timeout expired the response will be dropped.

ID	MCS00135772
Title	Deauth of AP during sl_stop is not always completed successfully.
Description	If sl_Stop is invoked when the device is connected to an AP, an internal disconnect command is executed. The device might shut down before the disconnection is complete.

ID	MCS00130040
Title	WiFi Direct Reliability: 65% Success rate when Peer device is initiator of connection
Description	Negotiation with other peer not always successful at first chance (fix increased to >90%)

ID	MCS00136304
Title	In some cases no re-calibration will be held after exit from shutdown
Description	Calibration was not executed due to wrong indication.

3.5 Fixed Items in previous package Version 1.0.0.10 SP 2.4.0.2.31.1.3.0.1.1.0.3.34

ID	MCS00133231
Title	SSL: Client Hello doesn't advertise SHA256 in the extension list
Description	Some servers requires SHA256 extension and will fail to connect if not present

ID	MCS00134065
Title	IOP: ActionTec AP Model: MI424-WR-GEN2 stops responding to DHCP discover
Description	When ActionTec AP is configured to WPA-TKIP, DHCP Server stops responding to DHCP Discover packets after x100 connections

ID	MCS00132679
Title	IOP: AP mode – System might halt when connected with a Linksys AE6000 station
Description	Linksys AE6000 sends corrupted packets while trying to connect to the device – the packets might halt the system.

ID	MCS00134538
Title	SSL: not able to connect with SHA-256 with some specific servers
Description	Fix for servers that sends a challenge request with SHA-256 (i.e www.dropbox.com)

ID	MCS00134809
Title	DHCP: The device might stop responding when changing DHCP client settings while it is connected to the Wi-Fi network
Description	After changing the DHCP setting (dynamic/static) the device must restarted in order for the configuration to take effect. The fix was to prevent the device from stop responding after the change of the settings (before restart)

ID	MCS00135125
Title	File System: Files above 500 KB can't be created in Fail Safe mode
Description	File size can be up to 1MB – the fix allow the fail-safe file to be up to 1MB as well.

	File that created by Uniflash require and updated version of it

ID	MCS00135183
Title	System Robustness: Improve start/stop robustness for SPI Big Endian
Description	Robustness issue observed after continuously performance start/stop fora ~10hours on system supporting Big Endian

ID	MCS00135236
Title	Host: General fixes
Description	Http server events fix Internal Spawn fixes SL Studio - use internal spawn by default

ID	MCS00135280
Title	WPS: System might halt if AP is disconnected
Description	In some rare cases when connecting to an AP using WPS the system might halt if the AP is been disconnected (reconfigured or shutdown)

ID	MCS00135328
Title	Host: false detection of sync pattern during read operation
Description	In some rare cases there might be a false detection of sync pattern during read operation

ID	MCS00134030
Title	Host: Blocking sl_Send with Tx size 0 prevents CW
Description	CW (continuous wave) didn't work if the Tx size was set to zero

ID	MCS00135346
Title	PM: NWP will not enter sleep due to packets that weren't released
Description	The NWP will not enter to sleep due to some DNS packets that weren't released

3.6 Errata - Known Issues

3.6.1 WiFi

ID	MCS00123349
Title	WiFi Security: CC3100 and CC3200 Supports only WEP with Key Index 0 (==> AP Key index 1)
Description	When using WEP security – only WEP index 0 is supported
Impact	Can't use more than one key in WEP security
Workaround	None

ID	MCS00106970
Title	WiFi Security: Traffic Stop while WPA EAP-TLS Enterprise and Reauthentication enabled
Description	In WPA EAP-TLS security the traffic stopped when Reauthentication packet is received
Impact	Traffic stopped
Workaround	Disabled Reauthentication or set it to a very long time

ID	MCS00131174
Title	Scan: Results list contain duplicate networks
Description	The SimpleLink might returns duplicate networks when the network list is not totally filled and the get scan results ask for fewer entries than what was actually found.
Impact	duplicate networks in Scan results list
Workaround	Read the maximum entries at once (20 entries) or to read one by one starting from the end to the beginning and check for duplicates. Once a duplicate was found the list is completed

3.6.2 WiFi - IOP

ID	MCS00135621
Title	IOP: Can't connect to MOXA AP configured to WPA-2
Description	The AP is publishing the EAPOL on QOS with wrong TID (not according to spec)
Impact	Can't connect with WPA-2
Workaround	Disable the WPA-2 or QOS
Remarks	Fix is Not Expected to the SimpleLink device FW upgrade to the AP is expected

ID	MCS00128381
Title	IOP: D-Link DWL 8600 AP - STA stops receiving Multicast traffic when WPA2 and key rotation are configured
Description	The AP is too busy transmitting the multicast frames, and tries to initiate the 2-way hand shake of the broadcast key rotation while SUT is in power save
Impact	The STA Stop receiving multicast traffic
Workaround	Disable Key Rotation in the AP
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128441
Title	IOP: Can't acquire DHCP IP address with 3COM WL-450 if security is configured to WPA2-AES
Impact	No IP address
Workaround	Configure the IP to static or disable security
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128156
Title	IOP: Connection to PCI MZK-MF300N doesn't complete when AP is configured to - Channel Width 40Mhz

Impact	No connection
Workaround	Configure the Channel Width to 20Mhz
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00130071
Title	IOP: Connection to Belkin F7D2301 v1 doesn't complete when AP is configured to - Channel Width 40Mhz
Impact	No connection
Workaround	Configure the Channel Width to 20Mhz
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128440
Title	IOP: D-Link DAP-2690. Low and unstable TCP Rx traffic due to AP not respecting 802.11 power save
Impact	Unstable traffic
Workaround	None
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00126520
Title	IOP: AP initiates deauth to the SL After ~5 Min of UDP Tx, when Remote PC is configured to 10M Full Duplex link speed
Description	Only in this network card configuration the AP sends deauth during the traffic
Impact	AP disconnected the STA during the UDP traffic
Workaround	Change the configuration of the network drive to Auto mode
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128462
Title	IOP: Linksys WAP55AG AP Is not compliant to 802.11 Power Save spec when configured to WAP2-AES
Impact	No Connection
Workaround	Disable security
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128725
Title	IOP: TRENDnet TEW-671BR – SL device doesn't respond to AP's frames at 11b rates
Impact	Can’t establish stable connection with the AP
Workaround	N/A

ID	MCS00128719
Title	IOP: TP-Link TD-W89841Nv4 AP. Is not compliant to 802.11 PS spec. Never asserts the Group bit in TIM IE
Description	AP never advertises the Group bit inside the TIM IE before and after transmitting of the ARP Request (broadcast packet) AP version: FW: 0.8.0 10.1 v0003.0 Build 121227 Rel.65166s

Impact	Can't Initiate Rx traffic
Workaround	Send Ping from the device to the AP after the connection
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128717
Title	IOP: Siemens Gigaset 01. Is not compliant to 802.11 PS spec. Never asserts the Group bit in TIM IE
Description	AP never advertises the Group bit inside the TIM IE before and after transmitting of the ARP Request (broadcast packet) AP version: FW: v1.0.0.1
Impact	Can't Initiate Rx traffic
Workaround	Send Ping from the device to the AP after the connection
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128462
Title	IOP: Linksys WAP55AG AP Is not compliant to 802.11 Power Save spec when configured to WAP2-AES
Description	AP doesn't Ack ARP response packets coming from the device when AES is enabled
Impact	Can't acquire IP when DHCP is enabled
Workaround	Disable AP security
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128703
Title	IOP: PCI MZK-MF300N AP. Is not compliant to 802.11 Power Save spec
Description	AP advertises the Group bit inside the TIM IE after transmitting of the ARP Request. SL device can't receive the packet AP version: FW: v1.00.05_B4
Impact	Can't Initiate Rx traffic
Workaround	Send Ping from the device to the AP after the connection
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128701
Title	IOP: I-O Data WN-G54/R4. Is not compliant to 802.11 Power Save spec
Description	AP advertises the Group bit inside the TIM IE after transmitting of the ARP Request. SL device can't receive the packet
Impact	Can't Initiate Rx traffic
Workaround	Send Ping from the device to the AP after the connection
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128693
Title	IOP: Netgear WNDAP350. Is not compliant to 802.11 Power Save spec
Description	AP advertises the Group bit inside the TIM IE after transmitting of the ARP Request. SL device can't receive the packet
Impact	Can't Initiate Rx traffic
Workaround	Send Ping from the device to the AP after the connection
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128607
Title	IOP: Netgear B90-7550. Is not compliant to 802.11 Power Save spec
Description	AP advertises the Group bit inside the TIM IE after transmitting of the ARP Request. SL device can't receive the packet
Impact	Can’t Initiate Rx traffic
Workaround	Send Ping from the device to the AP after the connection
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128606
Title	IOP: Belkin F7D5301v3. Is not compliant to 802.11 Power Save spec
Description	AP advertises the Group bit inside the TIM IE after transmitting of the ARP Request. SL device can't receive the packet
Impact	Can’t Initiate Rx traffic
Workaround	Send Ping from the device to the AP after the connection
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128367
Title	IOP: AP - STA Linksys AE1000 send NULL data with different sequence number
Description	When Linksys AE1000 dongle is connected to APUT, it sends NULL data with different sequence number than regular data. this yield to duplicated packet in the AP Rx side
Impact	Duplicated packet in AP Rx (mostly impact UDP)
Workaround	Disable AP security
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128672
Title	IOP: DLink DIR825 B1. UDP Rx Traffic is not Stable - AP stop transmitting Beacons after traffic starts
Description	At some point, AP stop transmitting Beacons, but does transmit data packets and RTS.
Impact	Traffic performance is not stable
Workaround	N/A
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00129371
Title	IOP: Netgear3700v1 AP - TCP Tx traffic doesn't Always start between two STA devices
Description	The AP doesn’t always forward the ARP Req if the STA was connect and disconnect for it number of times
Impact	Traffic doesn’t start
Workaround	The AP is stuck – need to restart
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00130102
Title	IOP: DLINK-615 With Security doesn't allow STA to fast reconnect
Description	The AP doesn’t allow fast reconnect without a formal de-authentication or long time out
Impact	Initial connection failed immediately upon reset Successful connection was established soon after

Workaround	Using the Fast and Auto Policy will insure the 2nd connection will work In Manual connection Disconnect before connect command solves the problem
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00130098
Title	IOP: WiFi Direct - Failure to connect as client to Galaxy S2
Description	With old versions of Galaxy S2 WiFi Direct – SimpleLink in client mode is not able to connect
Impact	Connection is not possible
Workaround	Switch the WiFi Direct policy to GO and enable Fast
Remarks	Fix is Not Expected due to WiFi Direct behavior

ID	MCS00129417
Title	IOP: Intellinet Wireless 3G Router. Is not compliant to 802.11 Power Save spec.
Description	AP advertises PVB wrongly before Action frame
Impact	In some cases can't Initiate Rx traffic
Workaround	Send Ping from the device to the AP after the connection
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00130025
Title	IOP: WiFi Direct - Re-Connection after SL device is client with Zopo device is unsuccessful
Description	Trying to disconnect and reconnect to a Zopo device is not successful if the SL device was a client
Impact	Re-Connection is not possible
Workaround	Switch the WiFi Direct policy to GO and enable Fast

ID	MCS00129759
Title	IOP: WPS - SL can't establish a WPS connection to the Actiontec PK5000 AP
Description	The AP is not excepting the WPS2.0 extension and refuse the connection
Impact	Can't connect with WPS
Workaround	Use other provisioning methods
Remarks	Fix is Not Expected (pending on SW upgrade to the AP)

3.6.3 Networking

ID	MCS00127876
Title	sl_NetAppDnsGetHostByName return with no answer in high traffic
Description	In high Rx traffic some DNS packets can get lost
Impact	No answer on request
Workaround	Run the API again

ID	MCS00128353
Title	UDP/RAW socket data payload is limited to MTU size
Description	Tx IP Fragmentation is not supported for UDP and RAW Tx
Impact	Packet bigger than MTU size will lead that portion of the packet will be discard

Workaround	Use packet size <= MTU size

ID	MCS00128580
Title	IOP: Microsoft MN-700 AP. Low Throughput Performance
Description	Throughput performance is low comparing to average throughout with other AP. The issue was also observed with other STA as well
Impact	Low Throughput Performance
Workaround	N/A
Remarks	Fix is Not Expected due to AP behavior

ID	MCS00128429
Title	IOP: Buffalo WZR-G300N AP. Low Rx Throughput Performance
Description	Rx throughput performance is lower comparing to average throughout with other AP
Impact	Low Throughput Performance
Workaround	N/A
Remarks	Fix is Not Expected due to AP behavior with aggregated packet in Rx

ID	MCS00119806
Title	IOP: Linksys WRT54gx v2 AP. Fails to obtain IP from DHCP server when operating with WPA2-PSK AES only privacy
Description	AP answers with a packet that is suspected as DHCP Offer, but this packet has MIC failure when decrypted, so the DHCP process is stuck
Impact	Connection is not feasible with WPA2-PSK AES and DHCP
Workaround	Use different security or disable DHCP
Remarks	Fix is Not Expected due to AP behavior during WPA2-PSK AES

ID	MCS00128959
Title	DHCP: SL continues using its previous IP address if an invalid IP in the DHCPACK (before lease time expired)
Description	DHCPACK arrives to SL with invalid address in the DHCPACK params address field but also the IP destination is the same invalid address (MAC address is the valid SL address). SL does not listen to other IPs address as destination but his own therefore this DHCPACK is not processed and SL continue to use his old address until the lease time expires
Impact	The device will continue to use the previous IP address
Workaround	N/A

ID	MCS00129407
Title	NS: SL device should discard ICMP Req datagram with problem in IP Header
Description	According to the RFC – if the gateway or host processing a ICMP Req datagram and finds a problem with the header parameters such that it cannot complete processing the datagram it must discard the datagram
Impact	Low impact – The SL device sends ICMP reply message
Workaround	N/A

ID	MCS00131564

Title	NS: Error -105 when trying to open 4 TCP server sockets while the internal HTTP server is running
Description	While the HTTP server is running one of the TCP server is been used and limit the number of user TCP Servers Error -105 - SL_ENOBUFS [No buffer space available]
Impact	Med impact – Only 3 TCP servers can be used while the HTTP is running
Workaround	Disable the internal HTTP Server if 4 TCP Server need to be used

ID	MCS00131966
Title	NS: blocking accept on secure socket doesn't return
Description	procedure: open secured socket bind listen select on socket => select not return when other side connected
Impact	High impact – Select doesn't return
Workaround	Don't use select method for accept on secure socket

ID	MCS00131612
Title	Transceiver mode: Can't configuring the channel of a RAW Socket if it's already open
Description	Changing the channel while a RAW socket is open to receive by using SetSockOpt command can halt the Host. The command response on SetSockOpt doesn't return. As a result, the host is might get stuck if it configured to blocking mode
Impact	Host might get stuck
Workaround	Close the socket and open it again with the correct channel

3.6.4 Host

ID	MCS00127283
Title	Free RTOS OS is not stable when running UDP traffic and Ping
Description	Known issue with free RTOS that can cause deadlock
Impact	Deadlock in OS
Workaround	Use TI RTOS

ID	MCS00130291
Title	WPS PIN Connect might fail if pin code is not null-terminated
Description	If the PIN code from the HOST is not null terminated the string can be wrongly used and in some cases the connection doesn't succeed
Impact	Connection doesn't succeed
Workaround	Add null termination to the PIN code string

3.6.5 Power Management

ID	MCS00128947

Title	In Enterprise network the device will Frequently Wakeup due to IPV4 BRDCST Rx frames
Description	On enterprise network there a lot of BRDCST packets
Impact	Increase in power consumption
Workaround	Add a filter to block the broadcast packets (will be different for each enterprise network)
Remarks	Fix is Not expected – the filter is specific to the network

3.6.6 Applications

ID	MCS00128652
Title	HTTP Server: When entering the internal web page with Huawei phone, GUI is zoomed in
Impact	Web page displayed incorrectly
Workaround	N/A

ID	MCS00128658
Title	HTTP Server: GUI is only displayed correctly after refresh in Nexus one phone
Impact	Web page displayed incorrectly
Workaround	N/A

ID	MCS00128130
Title	HTTP Server: With In Dolphin web application cursor is sometimes seen on two rows simultaneously
Impact	Double cursor
Workaround	N/A

ID	MCS00128425
Title	HTTP Server: Default Galaxy Tablet browser shows wrong authentication GUI
Impact	Wrong GUI is displayed
Workaround	Use different browser or disable authentication option

ID	MCS00129384
Title	HTTP Server: GUI - In IE7 browser, GUI boarder is truncated
Impact	Web page displayed incorrectly
Workaround	Use different browser
Remarks	Fix is Not Expected due to browser issue

ID	MCS00129385
Title	HTTP Server: On some mobile devices, "WiFi Connectivity" & "Profile Settings" are seen in two lines
Impact	Web page displayed incorrectly
Workaround	Use different browser
Remarks	Fix is Not Expected due to browser issue

ID	MCS00129390
Title	HTTP Server: On some mobile devices "some parameters were changed, System may require reset" is seen in two lines
Impact	Web page displayed incorrectly
Workaround	Use different browser
Remarks	Fix is Not Expected due to browser issue

ID	MCS00129392
Title	HTTP Server: On some mobile devices all tabs are merged together in browser
Impact	Web page displayed incorrectly
Workaround	Use different browser
Remarks	Fix is Not Expected due to browser issue

ID	MCS00129393, MCS00129394, MCS00129397, MCS00129399, MCS00129401
Title	HTTP Server: On some mobile devices lines and tabs are displayed incorrectly
Impact	Web page displayed incorrectly
Workaround	Use different browser
Remarks	Fix is Not Expected due to browser issue

ID	MCS00130155
Title	HTTP Server: Can't configure the Default Gateway from the HTTP Server pages (with default tokens)
Impact	When working with default HTTP server pages, only default gateway can be used (192.168.1.xxx)
Workaround	Add proprietary token to modify the default Gateway for user pages

ID	MCS00130240
Title	DNS Server: In AP mode the internal DNS Server can't be disabled
Impact	Can't disabled the internal DNS server – can't use external DNS server in AP mode
Workaround	DNS server in AP mode can't be disabled – It can be bypassed using IP UDP Raw socket and disable the DHCP server

ID	MCS00130241
Title	HTTP Server: 'AnyP2P' and 'Auto smart config' policies can be changed only in station or P2P mode
Impact	Can't change these specific configurations from the HTTP server in AP mode
Workaround	Change the configurations in STA mode

ID	MCS00131120
Title	HTTP Server: The System Up Time will get reset after 49Days
Impact	The displayed system up time won't be accurate after 49days
Workaround	Get Time from sl_DevGet SL_DEVICE_GENERAL_CONFIGURATION_DATE_TIME

ID	MCS00132268
Title	NetApp: the Ping response is sent to the Host only on timeout
Description	The Ping response is sent to the Host only on timeout and not when the response was

	actually received
Impact	Med impact – The Ping reply received very fast but the Host will have to wait few seconds until it will know that it received correctly
Workaround	Set pingCommand.Flags = 1 - this will return response for every ping

ID	MCS00131570
Title	HTTP Server: Version number displayed in hexadecimal instead of decimal
Description	The HTTP Pages display the SW version number in hexadecimal instead of decimal
Impact	Low impact – SW version is not displayed correctly
Workaround	Convert the version numbers to Dec in the HTTP page (user files)

ID	MCS00132159
Title	DHCP Server: Same address is provided if pool is full
Description	When all of the addresses in the DHCP server pool are assigned, it will continue to offer and assign the last address in the pool to new connected station
Impact	Low impact – The DHCP lease time is not kept for the last disconnected STA. Since only one client can connect at a time to the AP the STA will still get an IP and connect
Workaround	NA

ID	MCS00132200
Title	HTTP Server: SSID is limited to 16 characters
Description	From the HTTP web pages only the SSID string is limited to 16 characters instead of 32 characters
Impact	Med impact – Can’t add a SSID string longer than 16 characters from the HTTP using the device tokens
Workaround	Only the device tokens are limited – implementing user tokens for this field can overcome the issue

ID	MCS00132203
Title	HTTP Server: Password key is limited to 32 characters
Description	From the HTTP web pages only the password key is limited to 32 characters instead of 63 alphanumeric characters
Impact	Med impact – Can’t add a password key longer than 32 characters from the HTTP using the device tokens
Workaround	Only the device tokens are limited – implementing user tokens for this field can overcome the issue

ID	MCS00132206
Title	HTTP Server: Sending a page with no checkbox return "HTTP- No Content Length" message appears
Description	The internal web pages of the device returns "HTTP- No Content Length" if no checkbox is set
Impact	low impact – HTTP pages design
Workaround	Insuring that the form will never be empty by adding to the HTML form (that is sent via an HTTP POST) an additional input (can be set with type=hidden)

3.7 Migration from Host Driver Version 1.0.0.10 to Version 1.0.1.6

The new Host driver has some enhanced error handling mechanism including timeouts and error detection. To support the entire error handing mechanism, accurate timestamp service should be implemented in the Host application. This service is not mandatory. This section describes the minimal changes required in order to use the new version in applications that already running the old Host version (1.0.0.10).

3.7.1 Event handler

sl_GeneralEvtHdlr must be registered. This handler will enable the application to be notified on general/fatal driver errors and therefore it is mandatory. If the application already registered to this handler the handler should check for the new errors.

3.7.2 Spawn

In the new driver the spawn entry function returns a value. The spawn mechanism should be able to get a pointer to a function of the following type: typedef **short** (*_SlSpawnEntryFunc_t)(void* pValue);

3.7.3 Other

If the application is running on VisualStudio using the **SimpleLinkStudio** library, version 0.0.4.14 should be used with its new header files

Important Notice

Texas Instruments and its subsidiaries (TI) reserve the right to make changes to their products or to discontinue any product or service without notice, and advise customers to obtain the latest version of relevant information to verify, before placing orders, that information being relied on is current and complete. All products are sold subject to the terms and conditions of sale supplied at the time of order acknowledgement, including those pertaining to warranty, patent infringement, and limitation of liability.

TI warrants performance of its semiconductor products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are utilized to the extent TI deems necessary to support this warranty. Specific testing of all parameters of each device is not necessarily performed, except those mandated by government requirements.

CERTAIN APPLICATIONS USING SEMICONDUCTOR PRODUCTS MAY INVOLVE POTENTIAL RISKS OF DEATH, PERSONAL INJURY, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE ("CRITICAL APPLICATIONS"). TI SEMICONDUCTOR PRODUCTS ARE NOT DESIGNED, AUTHORIZED, OR WARRANTED TO BE SUITABLE FOR USE IN LIFE–SUPPORT DEVICES OR SYSTEMS OR OTHER CRITICAL APPLICATIONS. INCLUSION OF TI PRODUCTS IN SUCH APPLICATIONS IS UNDERSTOOD TO BE FULLY AT THE CUSTOMER'S RISK.

In order to minimize risks associated with the customer's applications, the customer to minimize inherent or procedural hazards must provide adequate design and operating safeguards.

TI assumes no liability for applications assistance or customer product design. TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right of TI covering or relating to any combination, machine, or process in which such semiconductor products or services might be or are used. TI's publication of information regarding any third party's products or services does not constitute TI's approval, warranty or endorsement thereof.