CC3100 SimpleLink™ Wi-Fi® Network Processor and Internet-of-Things Solution for MCU Applications

Software Development Kit (SDK) v1.2.0 Release Notes

TABLE OF CONTENTS

1 Introduction

This document describes the Software Development Kit (SDK) version 1.2.0 for use with the CC3100 SimpleLink Wi-Fi Network Processor device mounted on the CC3100 BoosterPack development platform.

2 Getting Started

Please follow the on-line CC3100 Quick Start Guide to start using the CC3100 BoosterPack development platform.

Please download the CC3100 Getting Started Guide to get started with your project development.

2.1 Procedure to Upgrade from SDKv1.1.0 to SDK1.2.0

To upgrade from SDKv1.1.0 to SDK1.2.0, servicepack_1.0.1.6.-2.6.0.5 needs to be flashed on CC3100. The servicepack_1.0.1.6.-2.6.0.5 is provided thru CC31xx_CC32xx_ServicePack-1.0.1.6-2.6.0.5 -windows-installer.exe downloadable from http://www.ti.com/tool/cc3100sdk. Please refer to UNIFLASH Quick start guide on details of flashing (http://processors.wiki.ti.com/index.php/CC31xx_%26_CC32xx_UniFlash) the service pack

3 Main changes from SDK 1.1.0

3.1 Networking

3.1.1 SSL – Domain Server name verification

Option to verify domain server name.

3.1.2 SSL – Support SHA384 on certificate chain verification

Enable SHA384 during certificate chain verification
As a server, the device is not supporting client authentication with SHA384 on the chain

3.1.3 SSL – Add support for new chipper suites in client mode

- 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

3.1.4 WiFi Enterprise security – Disable server authentication

Option to disable the server authentication using WiFi Enterprise security
Disabling authentication is available by using Wlan Connect command only (it is not kept in profiles)
Note: Disable need to be sent prior to every Wlanconnect command.

3.1.5 Reduce SFLASH access

Remove some write access to the SFLASH while exiting shutdown.

3.1.6 DHCP Enhancements

Improve the DHCP handshake robustness. Option to retrieve the DHCP lease time and default gateway address,

3.1.7 DNS Enhancements

- DNS enhancements were added to improve robustness.
  Enabling the option to temporarily set the amount of retries per DNS query.
- (For reference: 5 retries = ~1.5Sec, 11 retries = ~5Sec Default 32 retries = ~18Sec)
- Enabling the option to retrieve the secondary DNS server address and temporary set it.

3.1.8 Host Driver fixes and code optimizations

Allow easier integration with Network application libraries

- *Added Timeout mechanism –*
  - The driver has the ability to detect communications failures (timeouts) between the host and the SL device
  - This mechanism enables the driver to identify the timeouts and notify the application.
  - To enable this service, the application need to implement a function to get a timestamp and to register to the sl_GeneralEvtHdlr
- *Improved Error Indications*
  - The driver has the ability to detect and notify the application upon driver operations failures during SL API call that may cause the application to get stuck

- To get this service, the application need to register to the sl_GeneralEvtHdlr(user.h)

3.2 SDK Content

Please refer to Section 9 (Revision History) for changes in the SDK components.

4 Release Content

Item	Version	Type
Device	CC3100RES1.33 Chip Id : 0x4000000	Production device
Development boards	CC3100BOOST Rev3.3 onwards with CC31XXEMUBOOST Board Rev3.0	Orderable from TI
SDK Installer	CC3100SDK-1.2.0-windows-installer.exe For Windows 7	Provided with a click wrap license
Firmware	2.6.0.5.31.1.4.0.1.1.0.3.34	servicepack_1.0.1.6.-2.6.0.5 is provided thru ServicePack CC31xx_CC32xx_ServicePack -1.0.1.6-2.6.0.5-windows-installer.exe downloadable from http://www.ti.com/tool/cc3100sdk
Reference host platform	MSP430F5529 Launch Pad MSP430FR5969 Launchpad TM4C123GH6PM Launchpad TM4C1294NCPDT Launchpad	Orderable from TI
Network Processor Host driver	Version 1.0.1.6	Source code
Supported IDE	IAR version 6.20 for MSP430 IAR version 7.30 for TM4C CCS version 6.1 MS Visual Studio Express 2010 for PC & SimpleLink Studio Eclipse 4.3.0 for PC and SimpleLink Studio	Delivered separately
Demo	Embedded HTML web-site	Pre-flashed on Booster Pack and source code provided
User guides	CC3100 Getting started guide CC3100 BoosterPack User Guide SimpleLink Host Driver Programmer's Guide	PDF PDF Doxygen HTML
Tools	USB Drivers for CC31XXEMUBOOST board for Windows	Executable

5 Directory structure of SDK

Double-Click on the package to copy the directories (and files) to the preferred location. The first level directory structure is as shown in the table below.

Directory Name	Content
Docs	• Getting Started Guide for application development • Boards User Guide • SimpleLink Host Driver Programmer's Guide • Application notes for sample applications • MQTT library API document • HTTP client library API document • Simplelink OTA Extlib API document
Examples	Example application in source code
Netapps	• HTTP client library source code • MQTT library source code
Oslib	Interface file to configure Free-RTOS

Platform	• MSP430F5529lp
	  ○ CCS projects for all sample applications
	  ○ IAR projects for getting started applications
	  ○ Drivers
	  ○ Simplelink Host Driver Platform Configuration file (user.h)
	• TM4C123GH6PM, MSP430FR5969, TM4C1294NCPDT
	  ○ CCS and IAR projects for getting started applications
	  ○ Drivers
	  ○ Simplelink Host Driver Platform Configuration file (user.h)
	• simplelinkstudio:
	  ○ Visual-Studio Express and Eclipse projects for sample applications
	  ○ Simplelink Host Driver Platform Configuration file (user.h)

SimpleLink	• The SimpleLink Network Processor host driver code. • template_user.h file to be modified by the user for porting the driver to any host platform
Simplelink_extlib	OTA (over the air) library source code, Provisioning library
Third_party	Free-RTOS source code
Tools	**cc31xx_board_drivers:** USB Drivers for Windows 7 to enable application development on a PC using SimpleLink Studio for CC3100

6 Networking

6.1 Package Quality

6.1.1 Interoperability - IOP

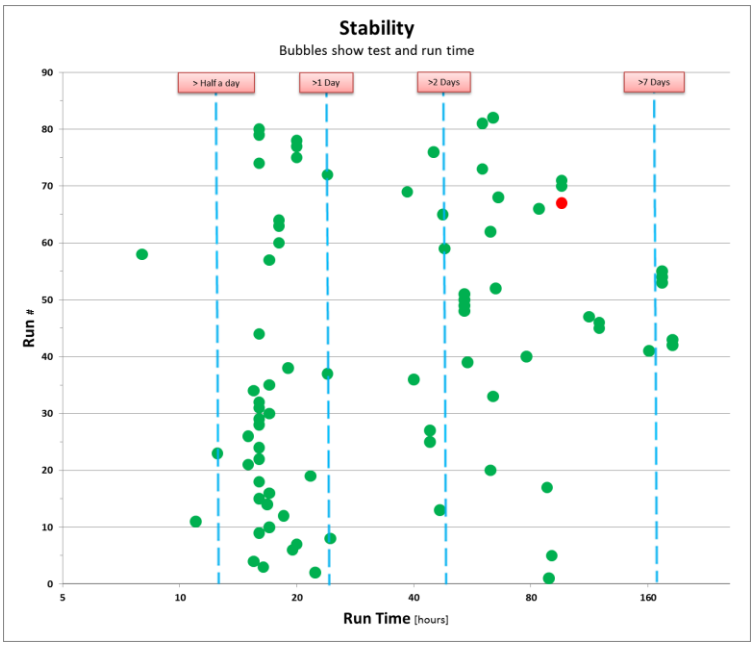
- STA mode was tested for connection, traffic and power consumption with more than 200 AP
- AP mode was tested for connection and traffic with more than 50 STA

6.1.2 Robustness

- Use cases were tests for 1000 of cycles – for example:
  - Connect/Disconnect
  - On/Off
  - Connect, Send Packet, Disconnect

6.1.3 Stability

- STA was kept running at different traffic scenarios in open AIR for long durations.
  - Green Dot - STA was stopped after a set time
  - The Failure tests (red dot) is representing TCP Tx with 163Byte payload in congested environment, the test fail due to socket disconnect after 67Hours (3 other instances passed >70hours)
-



6.2 Features

6.2.1 Wi-Fi

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

6.2.2 Networking protocols

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 TLSV1_2 TLS_RSA_WITH_AES_128_CBC_SHA256* TLSV1_2 TLS _RSA_WITH_AES_256_CBC_SHA256* TLSV1_2 TLS _ECDHE_RSA_WITH_AES_128_CBC_SHA256* TLSV1_2 TLS _ECDHE_ECDSA_WITH_AES_128_CBC_SHA256* *client mode
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)

6.2.3 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)

6.2.4 Interfaces

SPI	Standard SPI up to 20MHz on production device and up to 14MHz on Pre-Production device
UART	4 wire UART up to 3MHz

6.2.5 Power modes

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

7 Details

7.1 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

7.2 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

8 Sample applications

The release package includes sample applications created for the MSP430F5529 Launchpad including:

- Application Notes explaining the functionality usage
- Project file for IAR and CCS
- Smartphone application as needed

Some of the sample applications are also provided for MSP430FR5969, TM4C123GH6PM, TM4C1294NCPDT and SimpleLink Studio on a PC environment. All the applications can be easily ported to other MCUs and host processors. The default speed of SPI clock for MSP430F5529 is 12 MHz and can be increased to 20 MHz. Only debug configuration is provided for CCS and Visual Studio projects.

8.1 Antenna Selection

This is a reference implementation for antenna-selection scheme running on the host MCU, to enable improved radio performance inside buildings

8.2 Connection Policies

This application demonstrates the usage of the CC3100 profiles and connection-policies.

8.3 Send Email

This application sends an email using SMTP to a user-configurable email address at the push of a button.

8.4 Enterprise Network Connection

This application demonstrates the procedure for connecting the CC3100 to an enterprise network.

8.5 File System

This application demonstrates the use of the file system API to read and write files from the serial Flash.

8.6 Get Time

This application connects to an SNTP cloud server and receives the accurate time.

8.7 Get Weather

This application connects to ‘Open Weather Map’ cloud service and receives weather data.

8.8 Getting Started in AP Mode

This application configures the CC3100 in AP mode. It verifies the connection by pinging the connected client.

8.9 Getting Started in STA Mode

This application configures the CC3100 in STA mode. It verifies the connection by pinging the connected Access Point.

8.10 HTTP Client

This application demonstrates the use of HTTP client library API for HTTP based application development.

8.11 HTTP Server

This application demonstrates using the on-chip HTTP Server APIs to enable static and dynamic web page content.

8.12 IP Configuration

This application demonstrates how to enable static IP configuration instead of using DHCP.

8.13 MDNS

This application registers the service for broadcasting and attempts to get the service by the name broadcasted by another device.

8.14 Mode Configuration

This application demonstrates switching between STA and AP modes.

8.15 MQTT Client

This application showcase the use of MQTT library API to connect to an IBM MQTT broker and communicate using appropriate topic names.

8.16 NWP Filters

This application demonstrates the configuration of Rx-filtering to reduce the amount of traffic transferred to the host, and to achieve lower power consumption.

8.17 NWP Power Policy

This application shows how to enable different power policies to reduce power consumption based on use case in the station mode.

8.18 Out-of-box

This application demonstrates Out-of-Box experience with CC3100 Booster Pack

8.19 OTA sample application

This application focuses on showcasing CC3100's ability to receive firmware update and/or any related files over the internet enabled wifi interface. This example uses the Dropbox API app platform to store and distribute the OTA update files.

8.20 Wi-Fi Direct

This application configures the device in Wi-Fi Direct (P2P) mode and demonstrates how to communicate with a remote peer device.

8.21 Provisioning with WPS

This application demonstrates the usage of WPS Wi-Fi provisioning with CC3100.

8.22 Scan Policy

The application demonstrates the scan-policy settings in CC3100.

8.23 SPI Diagnostics Tool

This is a diagnostics application for troubleshooting the host SPI configuration.

8.24 SSL/TLS

The application demonstrates the usage of certificates with SSL/TLS for application traffic privacy and device or user authentication

8.25 TCP Socket

The application demonstrates simple connection with TCP traffic.

8.26 Transceiver Mode

The application demonstrates the CC3100 transceiver mode of operation.

8.27 UDP Socket

The application demonstrates simple connection with UDP traffic.

8.28 XMPP Client

The application demonstrates instant messaging using a cloud based XMPP server.

9 Revision History

SDK Version	Updates from previous version
1.2.0	• Bug fixes in Host SDK and NWP firmware • New simplelink provisioning library • Support for SSL Domain server name verification • SSL – SHA384 check during certificate chain authentication • Support for WiFi ENT security
1.1.0	• Added Support for Tiva connected (TM4C1294NCPDT) Launchpad (SPI interface) • Added HTTP client library and http_client sample application on MSP430F5529 LP • Added OTA library (simplelink_extlib) and ota sample application on MSP430F5529 LP • Added MQTT library and mqtt_client sample application on MSP430F5529 LP • Added Free RTOS on MSP430F5529 LP used by mqtt_client application. • Updated the platform depended files of MSP430 to build in GCC environment. • Removed file_download example • Removed support for MSP430F5529 Experimental board • Removed support for MSP430FR5739 Experimental board
1.0.0	• Adder support for MSP430FR5969 platform • Removing filters while configuring the device to default state • Added error handling in all the applications. • Moved AP and time configuration macro and networking status bit enum to common header file “sl_common.h” • Updated the “file_download” example to remove the use of temporary file • Modified uniflash session files to use the relative paths • Enabled automatic FTDI driver installation capability • Enabled FTDI driver support on 32 bit windows machine • Increased the SPI clock for all MCU platform
0.5.2	• Added a function to configure the firmware to default state across all applications. • Added error handling to Host driver API calls in application “Getting Started_in STA mode”. This can be used as sample reference code for writing new application.

	• Added CLI interface to MSP430F5529LP application to enable log prints.
0.5.1	First Release

10 Issues resolved in sample applications

Issue No.	1
Description	Mismatch in datatype of file descriptor when UART interface is used on MSP430F5529LP and Tiva-c-Launchpad.
Impact	Compilation warning/error while using the uart interface.

Issue No.	2
Description	Enabling Pull up on PB1 of Tiva-c platform before enabling the peripheral clock.
Impact	Tiva-c platform application project.

Issue No.	3
Description	CW (carrier wave) mode not working during transceiver mode
Impact	RadioTool CW mode testing will not work.

Issue No.	4
Description	Missing packet ID while sending the data over UDP socket
Impact	Iperf may recognize the packet as Out of Order.

11 Errata

The following section covers known issues and performance limitations with CC3100 production and pre-production devices.

11.1 Hardware

11.1.1 Pre-regulated 3.3v to Pin 47

For preproduction devices connect an external pre-regulated 3.3v +/- 5% supply to pin 47 (VDD_ANA2). This adds 12mA average current and up to 100mA peak current over 20uSec to the total system current at 3.3V.

The CC3100 BoosterPack version 3.3 already includes the correct supply configuration for the pre-production device and also adds a 10uF capacitor to filter the peak currents. No further action is required.

The external 3.3V supply is not required in the CC3100 production device in which case pin 47 should be left not connected.

11.1.2 Power consumption increase

Power consumption of the CC3100 pre-production device in all active modes is 1-2 mA higher compared to the CC3100 production devices

11.2 Performance

Item	Production device
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

11.3 Firmware issues fixed in this release

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	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

11.4 Fixed Items in this release (with respect to SP version 1.01)

ID	MCS00131961
Title	Scan: sl_WlanGetNetworkList does not return APs that their SSID contains only a single character
Description	AP with one character SSID are not presented in the Scan list. No problem to connect using explicitly command or profiles

ID	MCS00131623
Title	AP: SPI Big Endian Mode - missing Endianness conversion of the IP field in sl_NetCfgSet()
Description	In SPI Big Endian only sl_NetCfgSet() didn't worked correctly due to incorrect conversion in the code

ID	MCS00131560
Title	Host (SPI): Sync loss may occur after the Host is sending CNYS and wait for a long period of time before reading the response
Description	In case of the Read operation from the Host is been interrupted by a higher interrupt for a long duration the Host and device can get out of Sync – Interrupting the communication between the Host and Device in the middle of transaction should be avoided

ID	MCS00131573
Title	Host: Unsupported error codes appeared in wlan.h
Description	wlan.h contains list of error codes, which some of them are not supported.

ID	MCS00131575
Title	Host: sl_NetCfgGet might returns -2001 when getting the MACaddress of the device
Description	While getting the MAC address the NWP sends 8 bytes but the request was for 6 bytes (size of MAC). The result is trimmed to 6 bytes and error is returned although the value in the buffer contains the correct MAC address. Fix was provided in the Host Driver side.

ID	MCS00131717
Title	Host: Missing const qualifiers for some API parameters
Description	it's a common use case to have a const string in the code and pass it to functions

ID	MCS00131648
Title	Host: Driver may get stuck on ARC compiler by default due to inconsistency of

	volatile definition
Description	The ARC compiler has a non-standard mode on by default where any volatile variable is accessed as "uncached". This may cause issues if the same memory is accessed both as volatile pointer and without the volatile qualification as the compiler will access directly (bypassing the cache) on some accesses and through the cache on others (causing a cache coherency issue). The following data structures/pointers introduce this problem. g_pCB g_StatMem

ID	MCS00131508
Title	Host: Wrong command complete detection observed during HTTP_GETTOKEN_VALUE event handling
Description	wrong detection of the command complete can happen If the Host gets an HTTP_GETTOKEN_VALUE event after sending any command which requires a command complete response (and before its command complete received)

ID	MCS00131372
Title	Host: PlcpErrorPackets count definition has wrong meaning
Description	In SlGetRxStatResponse_t structure (wlan.h) the PlcpErrorPackets variable name was incorrectly used and renamed to AddressMismatchPacket in order to reflect the correct meaning

ID	MCS00131613
Title	File System: Updating a file while doing High traffic transfer in Rx transceiver mode can lead to a corruption of the file
Description	A file corruption can occur if traffic is been receiving in transceiver-mode socket while updating a file. The issue occur only in transceiver mode (disconnect)

ID	MCS00131703
Title	HTTP: TCP Timeout while constant access to the HTTP server
Description	A TCP socket timeout might happen due to traffic starvation caused by constantly accessing the internal HTTP

11.5 Wi-Fi known issues

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	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
Impact	The first connection doesn't success
Workaround	Try to connect again

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

11.6 Networking known issues

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	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

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
Impact	Undocumented error and the command is not taking any affect
Workaround	Program the setting in the image (Uniflash) and avoid using the API
Remarks	Fix is expected in the next service pack release

11.7 Host driver known Issues

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

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
Impact	Low impact – Certifications that are bounded by date will expire after year 2038
Workaround	N/A

11.8 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

11.9 Application

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)

12 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).

12.1.1 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.

12.1.2 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);

12.1.3 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