WINC1500 Software

Release Notes

VERSION : 19.5.3

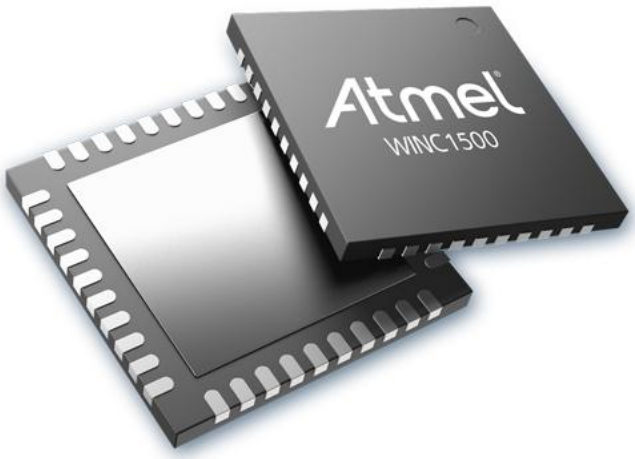
DATE : JULY 14 2017

Abstract

This document presents an overview of the WINC1500 software release version 19.5.3.

The following topics will be covered:

- Changes since previous release.
- Test information.
- New features & enhancements.



1. Introduction

This document describes the WINC1500 version 19.5.3 revision 15231 firmware release package. This is a release containing Wi-Fi functionality.

The release package contains all the necessary components (binaries and tools) required to make use of the latest features including documentation, tools, and firmware binaries.

The released firmware binary information is:

Firmware Version	19.5.3 revision 15231
Minimum driver version	19.3.0
SVN URL	trunk
Build date	Jul 13 2017 Time 17:01:51

2. Changes since the last release (version 19.5.2)

- WLAN Features:
  - Removed P2P (Wi-Fi direct) client mode feature.
  - AR (Auto Rate) algorithm improvements.
  - Add AP channel number in the connection info callback.
- Network Stack Features:
  - DHCP client improvements
  - Rate stuck at 1 Mbps issue fix.
  - TCP fast retransmission support.
- Various bug fixes.
  - Various Interoperability issues
  - Periodic NTP query failure
  - WINC1500 does not handle multiple DNS servers
  - PS bit is not set in ACK, CTS frames after power saving is turned off
  - WINC fails to re-connect to smartphone SoftAP
  - SSL connection failed for certificate with Expiry year in 2154
  - WINC misses m2m_wifi_connect right after M2M_WIFI_DISCONNECTED
  - DNS responses are parsed incorrectly if answer names are not compressed
  - WINC fails to HTTPS OTA from openssl secure server
  - Unable to receive broadcast packets when configured with Static IP
  - WINC hangs when receiving UDP packet with no data

The table below compares the features of 19.5.x to 19.4.4 release:

Features in 19.5.2	**Changes in 19.5.3**
Wi-Fi STA	
• IEEE 802.11 b/g/n. • OPEN, WEP security. • WPA Personal Security (WPA1/WPA2). • WPA Enterprise Security (WPA1/WPA2) supporting EAP-TTLS/MS-Chapv2.0 authentication with RADIUS server.	Same features + • Improved automatic rate selection algorithm for optimized TCP upload experience. • Support SAMW55 module. • Firmware does not print WLAN passcode in the WINC firmware log.
Wi-Fi Hotspot	
• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected. • OPEN and WEP, WPA2 security modes. • The device cannot work as a station in this	No change.

Features in 19.5.2	Changes in 19.5.3
mode (STA/AP Concurrency is not supported).	
Wi-Fi Direct	
• The device can operate only as a Wi-Fi Direct client (group owner function is not supported). • The device could not work as a station in this mode (STA/P2P concurrency is not supported).	Wi-Fi direct client is not supported.
WPS	
The WINC1500 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods.	No change
TCP/IP Stack	
The WINC1500 has a TCP/IP Stack running in firmware side. It supports TCP and UDP full socket operations (client/server). The maximum number of supported sockets is currently configured to 11 divided as: • 7 TCP sockets (client or server). • 4 UDP sockets (client or server).	Implement fast TCP re-transmission for improved TCP upload in busy radio environments.
Transport Layer Security	
• Support TLS v1.2. • Client and server modes. • Mutual authentication. • X509 certificate revocation scheme. • Add SHA384 and SHA512 support in X509 certificates processing. • Integration with ATECC508 (Add ECDSA/ECHE support). • Certificate revocation check API. • Disable Support of DH groups larger than 2048 bits. • Supported cipher suites are: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Fix an issue where SHA384 and SHA512 are not present in the list supported signature algorithms in the ClientHello message.

Features in 19.5.2	Changes in 19.5.3
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires ECC508) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires ATECC508)	
Networking Protocols	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2.	Fix DHCP client renew never timeout issue Add client identifier to DHCP request Various DHCP client improvements to confirm to RFC 2131
Power saving Modes	
• M2M_PS_MANUAL • M2M_PS_AUTOMATIC • M2M_PS_H_AUTOMATIC • M2M_PS_DEEP_AUTOMATIC	Improved initialization time (reduced by about 70ms)
Device Over-The-Air (OTA) upgrade	
	Improve WINC HTTPS client to allow it to work with HTTP servers which do not provide ‘content-length’ HTTP header field (e.g. openssl s_server).
Wi-Fi credentials provisioning via built-in HTTP server	
Built-in HTTP/HTTPS (TLS server mode) provisioning using AP mode (Open, WEP or WPA2 secured).	No change.
Ethernet Mode (TCP/IP Bypass)	
Allow WINC1500 to in WLAN MAC only mode and let the host to send/receive Ethernet frames.	No change.
ATE Test Mode	
Embedded ATE test mode for production line testing driven from the host MCU.	No change.

3. Test Information

This section summarizes the tests conducted for this release.

Testing was performed against the release candidate 19.5.3 revision 15231 against the following configuration(s):

H/W Version:	WINC1500 module
Host MCU:	ATSAMD21-XPRO
Test Request Info:	#9243

Testing was performed in both open air and shielded environments. The following testing has been performed:

- **General functionality.**
  - HTTP Provisioning.
  - Station Mode.
  - AP Mode.
  - IP Client (TCP and UDP).
  - IP Server (TCP and UDP).
  - Security (TLS).
  - WPS (PIN and PushButton methods).
  - Over-The-Air (OTA) update functionality.
  - Stability
  - Longevity.
  - Interoperability.
- **Performance under interference.**

4. Terms and Definitions

Term	Definition
ARP	Address Resolution Protocol
ASD	Application Specific Device
BLE	Bluetooth Low Energy
BSS	Basic Service Set
CPU	Central Processing Unit
CSPI	Configurable SPI
EAPOL	Extensible Authentication Protocol over LAN
e.g.	*exempli gratia*, for example
EEPROM	Electrically Erasable Programmable Read Only Memory
ESS	Extended Service Set (infrastructure network)
ESD	Electrostatic Discharge
Etc	*et cetera*, and the rest, and so forth
IC	Integrated Circuit
i.e.	*id est*, that is
IBSS	Independent BSS (ad-hoc network)
IEEE	Institute of Electronic and Electrical Engineers
MIB	Management Information Base
NDIS	Network Driver Interface Specification
OS	Operating System
OTA	Over The Air update
PCI	Peripheral Component Interconnect
PIN	Personal Identification Number
PMK	Pairwise Master Key
PSK	Pre-shared Key
QoS	Quality of Service
RSN	Robust Security Network
SPI	Serial Peripheral Interface
SSID	Service Set Identifier
RSSI	Receive Signal Strength Indicator
WEP	Wired Equivalent Privacy
Wi-Fi®	Wireless Fidelity (IEEE 802.11 wireless networking)
WLAN	Wireless Local Area Network
WMM™	Wi-Fi Multimedia
WMM-PS™	Wi-Fi Multimedia Power Save
WoWLAN	Wake On WLAN
WPA™	Wi-Fi Protected Access
WPA2™	Wi-Fi Protected Access 2 (same as IEEE 802.11i)

Atmel Corporation
1600 Technology Drive
San Jose, CA 95110
USA
Tel: (+1)(408) 441-0311
Fax:(+1)(408) 487-2600
www.atmel.com

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax:(+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax:(+49) 89-3194621

Atmel Japan G.K.
16F Shin-Osaki Kangyo Bldg.
1-6-4 Osaki, Shinagawa-ku
Tokyo 141-0032
JAPAN
Tel: (+81)(3) 6417-0300
Fax: (+81)(3) 6417-0370