ATWINC15x0 Software Release Notes

Release Overview

This document describes the ATWINC15x0 version 19.7.6 release package. The release package contains all the necessary components (binaries and tools) required for the latest features including tools, and firmware binaries.

Software Release Details

The following table provides the software release details.

Table 1. Software Version Information

Parameter	Description
Software Name	WINC15x0 Firmware
WINC Firmware Version	19.7.6
Host Driver Version	19.7.6
Minimum Driver Version	19.3.0

Release Impact

The newly added features in ATWINC15x0 v19.7.6 release are:

- Countermeasures for ‘Fragattack’ vulnerabilities
- Fix to TLS ALERT handling
- Improved gain tables for module antenna
- Transmit DC offset correction adjusted to optimal value
- Support for the WEP protocol is deprecated.

Notes:

1. For more information, refer to Wi-Fi Network Controller Software Design Guide (DS00002389).
2. For more details on release note information, refer to ASF firmware upgrade project doc folder.

Related Information

- Ordering Information
  - Customers who would like to order ATWINC15x0 with Firmware 19.7.6, contact Microchip marketing representative.
- Firmware Upgrade
  - To upgrade the ATWINC15x0-MR210xB module with the latest 19.7.6 release with ASF version 3.51, customers needs to follow the steps available in the salesforce knowledge base article:microchipsupport.force.com/s/article/How-to-update-WINC1500-module-to-19-7-6-release-using-ASF3-51.
  - Firmware 19.7.6 is supported in latest Harmony3. This is available for customers to update the ATWINC15x0-MR210xB module and supporting demo and evaluation boards.
    - Download the latest firmware package and driver from:github.com/Microchip-MPLAB-Harmony/wireless_wifi/
    - Download latest applications from: github.com/Microchip-MPLAB-Harmony/wireless_apps_winc1500

- Harmony 3 release notes available at github.com/Microchip-MPLAB-Harmony/wireless_apps_winc1500/blob/master/release_notes.md

Notes: The references to the ATWINC15x0-MR210xB module include the module devices listed in the following:

- ATWINC1500-MR210PB
- ATWINC1500-MR210UB
- ATWINC1510-MR210PB
- ATWINC1510-MR210UB

- Refer to the reference documents.

Note: For more information, refer to Microchip product webpage: www.microchip.com/wwwproducts/en/ATWINC1500.

Table of Contents

1. Release Details

1.1 Changes in Version 19.7.6, with respect to Version 19.7.3

The following table compares the features of 19.7.3 to 19.7.6 release.

Table 1-1. Comparison of Features between 19.7.3 and 19.7.6 Release

Features in 19.7.3	Changes in 19.7.6
Wi-Fi STA	
• IEEE802.11 b/g/n • OPEN, WEP security • WPA Personal Security (WPA1/WPA2) • WPA Enterprise Security (WPA1/WPA2) supporting : EAP-TTLSv0/MS-Chapv2.0 EAP-PEAPv0/MS-Chapv2.0 EAP-PEAPv1/MS-Chapv2.0 EAP-TLS EAP-PEAPv0/TLS EAP-PEAPv1/TLS	• Support for the WEP protocol is deprecated in 19.7.5. Attempts to configure it will result in error. • Countermeasures for ‘Fragattack’ vulnerabilities.
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 mode (STA/AP concurrency is not supported)	• Support for the WEP protocol is deprecated in 19.7.5. Attempts to configure it will result in error. • Countermeasures for ‘Fragattack’ vulnerabilities.
Wi-Fi Direct	
Wi-Fi direct client is not supported	No change
WPS	
The ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
TCP/IP Stack	
The ATWINC15x0 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)	No change
Transport Layer Security	

.....continued

Features in 19.7.3	Changes in 19.7.6

• Support TLS v1.2
• Client and server modes
• Mutual authentication in client mode.
• X509 certificate revocation scheme.
• SHA384 and SHA512 support in X509 certificates processing.
• Integration with ATECC508 (ECDSA and ECDHE support).
• 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`
`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 ATECC508)
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256` (requires ATECC508)
	• Fix to TLS ALERT handling

Networking Protocols	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2 SNTP	No change
Power saving Modes	
• M2M_PS_MANUAL • M2M_PS_DEEP_AUTOMATIC	No change
Device Over-The-Air (OTA) upgrade	
• Built-in OTA upgrade available • Backwards compatible as far as 19.4.4, with the exception of: – Wi-Fi Direct (removed in 19.5.3) – Monitor mode (removed in 19.5.2)	No change
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)	

.....continued	
Features in 19.7.3	**Changes in 19.7.6**
Allow ATWINC15x0 to operate in WLAN MAC only mode and let the host send/receive Ethernet frames.	No change
ATE Test Mode	
Embedded ATE test mode for production line testing driven from the host MCU	No change
Miscellaneous Features	
	• Improved gain tables for module antenna • Transmit DC offset correction adjusted to optimal value

1.2 Changes in Version 19.7.3, with respect to Version 19.6.1

The following table compares the features of 19.6.1 to 19.7.3 release.

Table 1-2. Comparison of Features between 19.6.1 and 19.7.3 Release

Features in 19.6.1	Changes in 19.7.3
Wi-Fi STA	
• IEEE802.11 b/g/n • OPEN, WEP security • WPA Personal Security (WPA1/WPA2) • WPA Enterprise Security (WPA1/WPA2) supporting : EAP-TTLSv0/MS-Chapv2.0 EAP-PEAPv0/MS-Chapv2.0 EAP-PEAPv1/MS-Chapv2.0 EAP-TLS EAP-PEAPv0/TLS EAP-PEAPv1/TLS	• Add WPA/WPA2 Enterprise option for TLS handshake certificate expiry checking mode
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 mode (STA/AP concurrency is not supported)	• Fix to ensure DHCP offered address is consistent when STA disconnects/ reconnects • Fix to close race condition when a STA disconnects and reconnects that could cause the WINC to disallow all fur-ther connection attempts.
Wi-Fi Direct	
Wi-Fi direct client is not supported	No change
WPS	
The ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
TCP/IP Stack	

.....continued

Features in 19.6.1	Changes in 19.7.3
The ATWINC15x0 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)	• Improvements to socket closing code • Improvements to TCP Rx windowing • Address “Amnesia” vulnerabilities
Transport Layer Security	

• Support TLS v1.2
• Client and server modes
• Mutual authentication in client mode.
• X509 certificate revocation scheme.
• SHA384 and SHA512 support in X509 certificates processing.
• Integration with ATECC508 (ECDSA and ECDHE support).
• 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`
`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 ATECC508)
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256` (requires ATECC508)
	• Added TLS ALPN support
	• Fix verification of certificate chains which include ECDSA signatures

Networking Protocols	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2 SNTP	• SNTP server allocated from DHCP is now cleared when switching between networks
Power saving Modes	
• M2M_PS_MANUAL • M2M_PS_DEEP_AUTOMATIC	No change
Device Over-The-Air (OTA) upgrade	

.....continued	
Features in 19.6.1	**Changes in 19.7.3**
• Built-in OTA upgrade available • Backwards compatible as far as 19.4.4, with the exception of: – Wi-Fi Direct (removed in 19.5.3) – Monitor mode (removed in 19.5.2)	No change
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 ATWINC15x0 to operate in WLAN MAC only mode and let the host send/receive Ethernet frames.	• Ensure broadcast frames contain correct destination MAC address • Ensure NULL frames are sent to keep the AP connection alive during periods of low activity.
ATE Test Mode	
Embedded ATE test mode for production line testing driven from the host MCU	No change
Miscellaneous Features	
	No change

1.3 Changes in Version 19.6.1, with respect to Version 19.5.4

The following table compares the features of 19.5.4 to 19.6.1 release.

Table 1-3. Comparison of Features between 19.5.4 and 19.6.1 Release

Features in 19.5.4	Changes in 19.6.1
Wi-Fi STA	
• IEEE802.11 b/g/n • OPEN, WEP security • WPA Personal Security (WPA1/WPA2) • WPA Enterprise Security (WPA1/WPA2) supporting EAP-TTLSv0/MSCHAPv2 authentication with RADIUS server	Same features along with the following: • WPA/WPA2 Enterprise new methods: – EAP-PEAPv0/MSCHAPv2 – EAP-PEAPv1/MSCHAPv2 – EAP-PEAPv0/TLS – EAP-PEAPv1/TLS – EAP-TLS • WPA/WPA2 Enterprise other new features – Phase 1 TLS session caching – Option to specify domain – Option to send actual identity in phase 1 • Simple Roaming support • Improved connection API, allowing connection via BSSID as well as SSID • Option to encrypt connection credentials that are stored in ATWINC15x0 flash

.....continued	
Features in 19.5.4	**Changes in 19.6.1**
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 mode (STA/AP concurrency is not supported)	No change
Wi-Fi Direct	
Wi-Fi direct client is not supported	No change
WPS	
The ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
TCP/IP Stack	
The ATWINC15x0 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)	No change
Transport Layer Security	

.....continued

Features in 19.5.4	Changes in 19.6.1

• Support TLS v1.2
• Client and server modes
• Mutual authentication
• Custom scheme for X509 certificate revocation
• X509 certificate support including SHA1, SHA256, SHA384 and SHA512
• Integration with ATECC508 (adds support for ECDSA/ECHE)
• 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`
`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 ATECC508)
`TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256` (requires ATECC508)
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256` (requires ATECC508)
	No change

Networking Protocols	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2 SNTP	SNTP servers are fully customizable
Power saving Modes	
• M2M_PS_MANUAL • M2M_PS_AUTOMATIC • M2M_PS_H_AUTOMATIC • M2M_PS_DEEP_AUTOMATIC	No change
Device Over-The-Air (OTA) upgrade	
• Built-in OTA upgrade available • Backwards compatible as far as 19.4.4, with the exception of: – Wi-Fi Direct (removed in 19.5.3) – Monitor mode (removed in 19.5.2)	No change

.....continued	
Features in 19.5.4	**Changes in 19.6.1**
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)	• Improved provisioning user experience • Default gateway and subnet mask can now be customized when in AP mode
Ethernet Mode (TCP/IP Bypass)	
Allow ATWINC15x0 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
Miscellaneous Features	
	• Addition of host file download capability, allowing the host MCU to download and retrieve files from the ATWINC1510 flash • Multiple Gain Table support - Support upto 4 gain tables • Simple Roaming feature • Encrypted credential storage in ATWINC15x0 flash

1.4 Changes in Version 19.5.4, with respect to Version 19.5.3

The following table compares the features of 19.5.3 to 19.5.4 release.

Table 1-4. Comparison of Features between 19.5.3 and 19.5.4 Release

Features in 19.5.3	Changes in 19.5.4
Wi-Fi STA	
• IEEE802.11 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	• Protect against key re-installation attacks forcing NONCE re-use • Fix `m2m_wifi_set_tx_power()` to work in all cases • Fix interoperability issues with ARRIS TG862G/CT (Xfinity) access point
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 mode (STA/AP concurrency is not supported)	No change
Wi-Fi Direct	
Wi-Fi direct client is not supported	No change
WPS	

.....continued

Features in 19.5.3	Changes in 19.5.4
The ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
TCP/IP Stack	
The ATWINC15x0 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)	No change
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`
`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 ATECC508)
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256` (requires ATECC508)
	No change

Networking Protocols	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2 SNTP	Use NTP server pools instead of specific servers
Power saving Modes	

.....continued	
Features in 19.5.3	**Changes in 19.5.4**
• M2M_PS_MANUAL • M2M_PS_AUTOMATIC • M2M_PS_H_AUTOMATIC • M2M_PS_DEEP_AUTOMATIC	No change
Device Over-The-Air (OTA) upgrade	
• Built-in OTA upgrade available • Backwards compatible as far as 19.4.4, with the exception of: – Wi-Fi Direct (removed in 19.5.3) – Monitor mode (removed in 19.5.2)	No change
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 ATWINC15x0 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

1.5 Changes in Version 19.5.3, with respect to Version 19.5.2

The following table compares the features of 19.5.2 to 19.5.3 release.

Table 1-5. Comparison of Features between 19.5.2 and 19.5.3 Release

Features in 19.5.2	Changes in 19.5.3
Wi-Fi STA	
• IEEE802.11 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 along with the following: • Improved automatic rate selection algorithm for optimized TCP upload experience • Supports 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 mode (STA/AP concurrency is not supported)	No change
Wi-Fi Direct	

.....continued

Features in 19.5.2	Changes in 19.5.3
• 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 ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
TCP/IP Stack	
The ATWINC15x0 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`
`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 ATECC508)
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256` (requires ATECC508)
	Fix an issue where SHA384 and SHA512 are not present in the list supported signature algorithms in the ClientHello message

Networking Protocols	

.....continued	
Features in 19.5.2	**Changes in 19.5.3**
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 70 ms)
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 ATWINC15x0 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

1.6 Changes in Version 19.5.2, with respect to Version 19.4.4

The following table compares the features of 19.4.4 to 19.5.2 release.

Table 1-6. Comparison of Features between 19.4.4 and 19.5.2 Release

Features in 19.4.4	Changes in 19.5.2
Wi-Fi STA	
• IEEE802.11 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	No change
Wi-Fi Hotspot	
• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected • OPEN and WEP security modes • The device cannot work as a station in this mode (STA/AP concurrency is not supported)	Added WPA/WPA2 security mode

.....continued

Features in 19.4.4	Changes in 19.5.2
WPS	
The ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
TCP/IP Stack	
The ATWINC15x0 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)	No change
Transport Layer Security	

• TLS protocol version 1.0 TLSv1.0
• TLS v1.2 Client operation only
• RSA is the only supported Public Key Algorithm with AES and is the only supported Encryption technique
• Supported cipher suites are:
`TLS_RSA_WITH_AES_128_CBC_SHA`
`TLS_RSA_WITH_AES_256_CBC_SHA`
`TLS_RSA_WITH_AES_128_CBC_SHA256`
`TLS_RSA_WITH_AES_256_CBC_SHA256`
	• 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`
	`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 ATECC508)
	`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256` (requires ATECC508)

Networking Protocols	

.....continued	
Features in 19.4.4	**Changes in 19.5.2**
DHCPv4 (client/server) DNS Resolver IGMPv1, v2	Add device name feature in DHCP requests
Power saving Modes	
• M2M_PS_MANUAL • M2M_PS_AUTOMATIC • M2M_PS_H_AUTOMATIC • M2M_PS_DEEP_AUTOMATIC	Same list of power saving modes. Optimized power saving state machine which reduced power consumption during: • Idle disconnected • Beacon monitoring • Intermittent traffic
Device Over-The-Air (OTA) upgrade	
Wi-Fi credentials provisioning via built-in HTTP server	
Built-in HTTP provisioning using AP mode	HTTPS support (needs TLS server) on WPA2 secured AP mode
Ethernet Mode (TCP/IP Bypass)	
Allow ATWINC15x0 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

1.7 Version 19.4.4, Initial Release

Initial release of version 19.4.4 to public.

2. Known Problems and Solutions

The following table provides the list of known problems and solutions.

Additional known issues information can be found at github.com/MicrochipTech/WINC15x0-known-issues

Table 2-1. Known Problems and Solutions

Problem	Solution
Occasionally ATWINC15x0 fails to receive an individual UDP broadcast frame when in M2M_PS_DEEP_AUTOMATIC powersave mode.	Use M2M_NO_PS Power Save mode if reliability is preferred for UDP broadcast frames. Otherwise ensure the overlying protocol can handle the odd missing frame.
The ATWINC15x0 cannot handle two simultaneous TLS handshakes, due to memory constraints.	When attempting to open two secure sockets in STA mode, the application should wait to be notified of the first one completing (succeeding or failing) before attempting the second one.
1% of Enterprise conversations fail due to the ATWINC15x0 not sending an EAP response. The response is prepared and ready to send but does not appear on the air. After 10 seconds the firmware times-out the connection attempt and the application is notified of the failure to connect.	Configure the authentication server to retry EAP requests (with interval < 10 seconds). The application should retry the connection request when it is notified of the failure.
When connected to certain access points, the ATWINC15x0 sometimes fails to roam when the access point changes channel. The issue is seen with these access points: Linksys E2500, Linksys E4200, Linksys 6500. The failures to roam are due to two issues: • Sometimes the access point takes a long time to start sending beacons or probe responses on the new channel, so it is not discoverable. • Sometimes the access point does not initiate the 4-way handshake (for WPA/WPA2 PSK reconnection).	On reception of M2M_WIFI_DISCONNECTED event, the application should attempt to discover the access point using `m2m_wifi_request_scan()` API.
If an AP uses an 802.11 ACK policy of “No Ack”, then the ATWINC15x0 sometimes fails to receive 802.11b frames.	Avoid using an ACK policy of “No Ack”. If “No Ack” is used, ensure frames are sent at 802.11g or higher rates.
70% of Enterprise connection requests fail with a TP Link Archer D2 access point (TPLink-AC750-D2). The access point does not forward the initial EAP Identity Re-sponse to the authentication server. The issue is bypassed by PMKSA caching (WPA2 only), so reconnection attempts will succeed.	The application should retry the connection request when it is notified of the failure.
Occasionally during AP provisioning, after entering the credentials of the AP to connect to and pressing “connect”, an error will be returned even though provisioning was suc-cessful and the connection proceeds.	Add a delay in the application between receiving the provisioning info and con-necting to the AP. Ignore the “Request Failed” message
Using TLS Server mode with a server certificate that is signed with a key size which differs from the key size contained within the certificate can cause the WINC to crash.	Only use a TLS Server certificate that is signed using the same key size as the key contained within the certificate.

.....continued	
Problem	**Solution**
When using a driver pre – 19.6.0 with this firmware, upon failure to obtain a DHCP ad-dress the WINC will not trigger a WiFi Disconnection and notify the driver of the failure.	In this case of an older driver running with later firmware, the application should monitor the time taken to obtain a DHCP address, if it takes too long then it can decide whether to disconnect and try again.

The Microchip Web Site

Microchip provides online support via our web site at www.microchip.com/. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Customer Change Notification Service

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at www.microchip.com/. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Trademarks

ISBN:

Quality Management System Certified by DNV

ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4450-2828 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-67-3636 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-7289-7561 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820