

# smxWiFi™

## 802.11 MAC

*smxWiFi is a robust 802.11 Media Access Control (MAC) stack specifically designed and developed for embedded systems. It is written in C and can run on any hardware platform. While optimized for SMX®, smxWiFi can be ported to another RTOS or to another hardware platform to support a different Wi-Fi chipset.*

An 802.11 network is a wireless local area network (WLAN) that conforms to the 802.11 standards. smxWiFi provides the necessary software to add wireless connectivity to an embedded system.

### Layers

- **Network Interface Layer** Provides the interface to a TCP/IP stack.
- **Application Interface Layer** Provides the interface to the application to manage the networking connection, retrieve the signal and link quality information, and do a site survey.
- **MLME Layer** Provides services for the MAC Layer Management Entity, such as scan, authentication, association, and synchronization.
- **Chipset Driver Layer** Provides a unique interface for different Wi-Fi MAC and RF chipsets such as the Ralink RT3572.
- **Porting Layer** Provides service functions related to the hardware, OS, and compiler.

Due to the complexities of the 802.11 protocol, smxWiFi requires a multitasking RTOS environment. It is integrated with SMX. A TCP/IP stack is also required, and smxWiFi

### Features

- Supports 802.11a/b/g/i/n.
- Supports both *Infrastructure* (connection to an AP) and *Independent BSS* (ad hoc peer to peer connection). Hidden AP is also supported.
- Supports SoftAP.
- Supports Wi-Fi Peer-to-Peer (P2P).
- Supports Wi-Fi Simple Configuration. Both PBC and PIN are supported.
- Supports Enterprise security and RADIUS server through PEAP/MSCHAPv2.
- Supports Open, Shared, 802.11i authentication types.
- Supports WEP, TKIP and AES encryption modes.
- Supports the MediaTek MT7601, Ralink RT2573, RT2860, RT2870, RT3070, RT3572, RT5370, and RT5572 chipsets.
- Dynamic selection of chipset driver when multiple purchased.
- Interfaced to smxNS. Easily portable to other TCP/IP stacks.
- Interfaced to smxUSBH for USB Wi-Fi dongle support.
- Also supports PCI Wi-Fi cards.
- Written entirely in ANSI-C.
- Optimized for SMX® RTOS. Easily portable to other RTOSs.

has been integrated with smxNS. To support USB dongles, a USB host stack is required, such as smxUSBH (strongly recommended).

## Optional Features

See the smxWiFi User's Guide for limitations of these features.

**SoftAP** provides simple Access Point functionality to allow connection of Wi-Fi devices.

**Wi-Fi Peer-to-Peer (P2P)** allows easy, direct connection among Wi-Fi devices, anywhere. There is no need for an Access Point. It is a protocol designed to replace the legacy ad-hoc (IBSS) protocol. Improvements over ad-hoc include easier connection and the latest security, 802.11i. As with any Wi-Fi device, the range is up to 200m, making connection convenient even when devices are not in immediate proximity to one another. When used with SoftAP, it allows the device to be the Group Owner, else only a client.

**Wi-Fi Simple Configuration** simplifies connection to an AP or other device. It is required by P2P.

## Types of Security

There are two parameters for security. One is the Authentication Type and the other is the Encryption Algorithm/Protocol.

### Authentication Types include:

Open System: There is no special authentication. Any Wi-Fi stations can connect to each other.

Shared Key: An old Authentication type, only used with WEP.

WPA: Wi-Fi Protected Access. This is a working standard put together by the Wi-Fi Alliance. It is based on 802.11i draft version.

WPA-PSK: WPA Personal. Based on 802.11i pre-shared key authentication.

WPA-EAP: WPA Enterprise. Uses the authenticated key mode that derives keys from 802.1X.

WPA2: WPA version 2. It is the same as 802.11i.

WPA2-PSK: Same as WPA-PSK but for WPA version 2 (802.11i)

WPA2-EAP: Same as WPA-EAP but for WPA version 2 (802.11i).

### Encryption Protocols include:

WEP: Wired Equivalent Privacy. This is the first Wi-Fi encryption algorithm, based on RC4. There are two key lengths, 64-bit and 128-bit

TKIP: Temporal Key Integrity Protocol. This encryption protocol is still based on RC4 but some improvements were made, such as adding message integrity check (MIC).

AES: Advanced Encryption Standard, also called Counter Mode with CBC-MAC Protocol (CCMP).

When discussing Wi-Fi security, we combine these two components together. For example: WEP64 means we use shared key authentication and WEP 64-bit encryption. WEP128 means we use shared key authentication and WEP 128-bit encryption. WPA-PSK/AES means we use WPA-PSK authentication and AES encryption protocol.

## Code Size

Component	ARM Th2 IAR (KB)	ARM IAR (KB)	CF CW (KB)
Core Stack 802.11abg	30.5	47.5	53.0
802.11n	4.0	7.5	7.5
Security (WEP + WPA)	21.5	27.5	25.0
Enterprise	58.0	92.5	106
Peer-to-Peer (P2P)	57.0	82.0	

Simple Config (WSC)	24.0	38.0	49.0
SoftAP	12.0	20.0	
MediaTek MT7601	76.0	90.0	
Ralink RT2573	20.5	23.0	31.0
Ralink RT2870	31.5	37.0	44.0
Ralink RT3070	34.5	40.0	49.0
Ralink RT3572	32.5	39.0	47.0
Ralink RT5370	43.5	50.0	61.0
Ralink RT5572	36.0	46.0	55.0

The payload size of the UDP packet is 1472. TCP packet size is 64KB. Code is in wifidemo.c.

<b>Board</b>	<b>UDP send</b>	<b>TCP send</b>
AT91SAM9M10 (400MHz EHCI)	11900 KB/s (95Mbps)	6300 KB/s (50Mbps)

## Data Size

<b>Component</b>	<b>Size (KB)</b>
Core Stack 802.11abg	9
802.11n	2
Security (WEP + WPA)	4
Enterprise	5
Peer-to-Peer (P2P)	4
Simple Config (WSC)	2
SoftAP	2+2*ncli
MediaTek MT7601	12
Ralink RT2573 Driver	8
Ralink RT2870 Driver	12
Ralink RT3070 Driver	12
Ralink RT3572 Driver	12
Ralink RT5370 Driver	12
Ralink RT5572 Driver	12

## Porting

smxBase has definitions, macros, and functions to port smxWiFi to a particular target, such as another compiler and RTOS. In addition, if the Wi-Fi chipset is not already supported, a new driver will need to be written.

smxWiFi was developed for use with SMX<sup>®</sup> and smxNS, but it can be ported to another RTOS and TCP/IP stack. Use of smxUSBH is recommended, since porting to another USB host stack is challenging.

## Performance

For performance testing, UDP/TCP packets are sent from the AT91SAM9M10G45-EK board. Instruction and data cache of the processor are enabled. iPerf was running at the Windows host side to measure the performance.

Wi-Fi performance highly depends on the environment and the device being used. The AP used was Linksys E4200, which works for 11n only and uses 5GHz Channel 44. There were no other APs using any 5GHz channel during the testing. An RT5372 dual band USB dongle was used as the Wi-Fi device.

## smxWiFi API

swf\_Init()  
swf\_Open()  
swf\_Close()  
swf\_Release()  
  
swf\_RegisterNotify()  
swf\_GetNodeID()  
swf\_SendPacket()  
swf\_GetLinkStatus()  
swf\_Connect()  
swf\_Disconnect()  
swf\_IsConnected()  
swf\_IsInserted()  
swf\_IsOpen()  
swf\_ScanBss()  
swf\_GetBssNum()  
swf\_GetBssInfo()  
swf\_SetBssType()  
swf\_SetAdhocChannel()  
swf\_SetPowerSaveMode()  
  
swf\_SetAuthMode()  
swf\_SetWepDefaultKeyID()  
swf\_SetWepSharedKey()  
swf\_GenerateWPAKey()  
swf\_SetWPAKey()  
swf\_SetEAPCredentials()  
swf\_WPSStartPBC()  
swf\_WPSStartPIN()  
swf\_WPSGeneratePIN()

## Tested Devices

### Wi-Fi Dongles/Cards

- AmbiCom M600N-USB (RT2870)
- AmbiCom WL150N-nUSB (RT3070)
- AmbiCom WL150N-USBx (RT3070)
- Asus USB-N13 (RT3072)
- Belkin F5D7050 v3002 (RT2573)
- Belkin F5D8053 v3001 (RT2870)
- Buffalo WLI-UC-G300N (RT2870)
- D-Link DWA-140 (RT2870)
- D-Link EWUGRL2700 (RT2573)
- Linksys AE1000 (RT3572)
- Linksys WUSB54GC (RT2573)
- Linksys WUSB54GC v3 (RT3070)
- Linksys WUSB600N ver.2 (RT3572)
- MediaTek 7601 (MT7601)
- Ralink 2070 (RT2573)
- Ralink 3070 WS-WNU682N (RT3070)
- Ralink 5370 OEM dongle (RT5370)
- Samsung, WIS09ABGN LinkStick USB Adapter (RT2870)
- SparkLAN WUBR-170GN dongle (RT3370)
- SparkLAN WUBR-507N dongle (RT3572)
- SparkLAN WUBR-508N dongle (RT5572)
- W483 802.11n PCI Card (RT2860)

### RADIUS Servers

- Cisco ACS v5.2
- FreeRadius Server v2.1.10 on Fedora 13
- ZyXEL NWA3160-N Built-In Radius Server

## **Access Points**

- Apple AirPort Extreme A1034 Router
- Apple AirPort Extreme A1354 802.11n Router
- Belkin N150 Wireless Router
- Cisco 861W Router
- Cisco AIR-AP1262N-A-K9
- D-Link DIR-601 Router
- D-Link DIR-615 Router
- D-Link DIR-625 RangeBooster N Router
- D-Link DIR-655 Extreme N Router
- FRITZ!Box Fon WLAN 7270
- Linksys E1200 Wireless-N Router
- Linksys E4200 Wireless-N Router
- Linksys E4500 Wireless-N Router
- Linksys WRT54G Wireless Router
- Linksys WRT160N Wireless-N Router
- Linksys WRT320N Dual-Band Wireless-N Router
- Linksys WRT400N Dual-Band Wireless-N Router
- NETGEAR WGR614 v6 Wireless Router
- NETGEAR WNDR3300 RangeMax Dual Band Wireless-N Router
- NETGEAR WNR2000 N300 Wireless Router
- TP-Link TL-WR841ND Wireless N Router

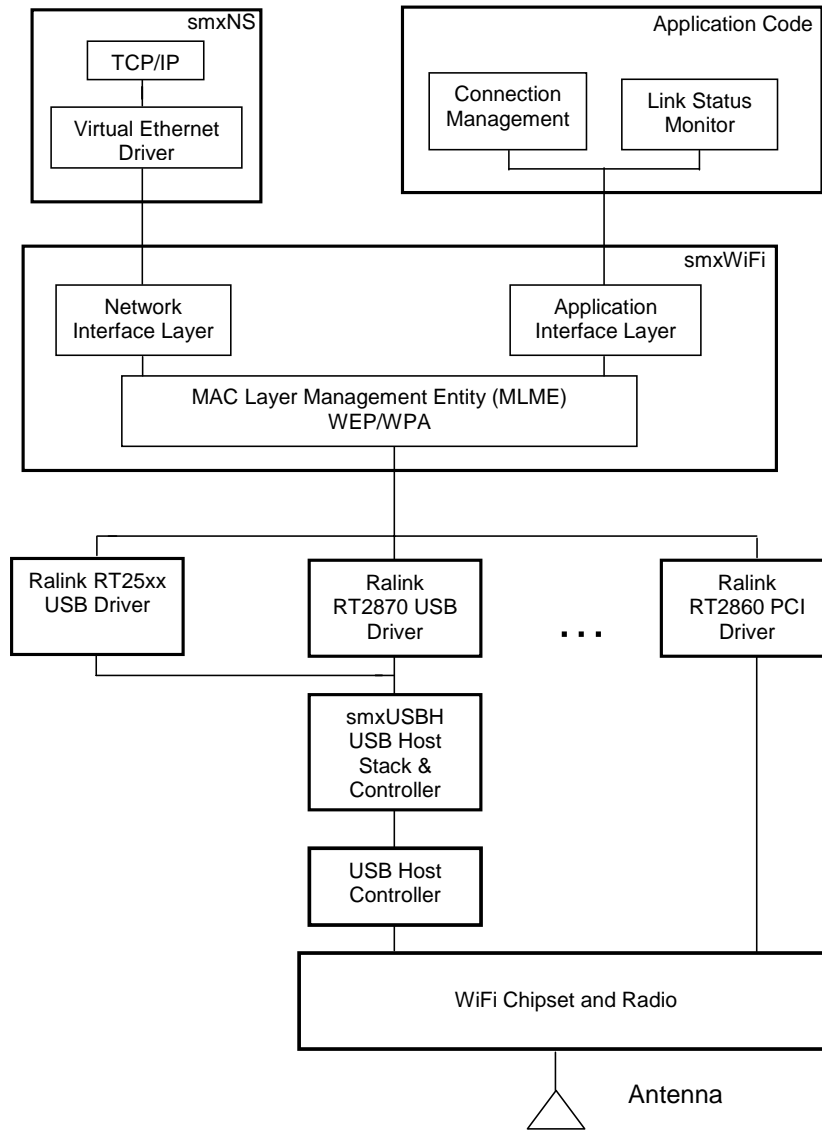
- TRENDnet TEW-432BRP 11g Wireless Router

## **Clients for SoftAP**

- Android 4.0.4, 4.1, 4.2.2 Samsung Note Tablet and Phone
- Android 4.2.2 Asus Memo 7 HD Tablet
- Apple iBook G4 laptop OS X 10.5.8
- iPad 2nd Generation iOS 6.0
- Linux with with Ralink Wi-Fi chipset driver
- Microsoft Windows with Ralink, Realtek, and Atheros Wi-Fi chipset driver

## **Wi-Fi Peer-to-Peer (P2P) Devices**

- Android 4.0.4, 4.1, 4.2.2 Samsung Note Tablet and Phone
- Android 4.2.2 Asus Memo 7 HD Tablet
- Netgear Push2TV3000



See [www.smxrtos.com/wificert.htm](http://www.smxrtos.com/wificert.htm) to learn how protocols supported by smxWiFi correspond to the certification programs of Wi-Fi Alliance, such as Wi-Fi Direct™, Wi-Fi Protected Setup™, Wi-Fi Protected Access®, WPA™, and WPA2™.