

SPA Computers (P) Ltd.

Wireless Access Point Features

(IEEE 802.11 a/b/g)

Wireless Access Point Standard

Article I. IEEE 802.11 - Overview

802.11 Task Groups

The task groups of the 802.11 standard are:

- 802.11a - Created a standard for WLAN operations in the 5 GHz band, with data rates of up to 54 million bits per sec (Mbps). Published in 1999. One of the company using this standard is Atheros (<http://atheros.com/>).
 - 802.11b - Created a standard (also known as Wi-Fi) for WLAN operations in 2.4 GHz band, with data rates of up to 11 Mbps. Published in 1999. Products based on 802.11b include public space Internet kiosks.
 - 802.11c - Provided documentation of 802.11-specific MAC procedures to the ISO/IEC (International Organization for Standardization/International Electro Technical Commission) 10038 (IEEE 802.1D) standard.
 - 802.11d - Publishing definitions and requirements to allow the 802.11 standard to operate in countries not currently served by the standard.
 - 802.11e - Attempting to enhance the 802.11 MAC to increase the quality of service possible. Improvement in capabilities and efficiency are planned to allow applications such as voice, video, or audio transport over 802.11 wireless networks.
 - 802.11f - Developing recommended practices for implementing the 802.11 concepts of Access Points and Distribution Systems. The purpose is to increase compatibility between Access Point devices from different vendors.
 - 802.11g - Developing a higher-speed PHY extension to the 802.11b standard, while maintaining backward compatibility with current 802.11b devices. The target data rate for the project is at least 20 Mbps.
 - 802.11h - Enhancing the 802.11 MAC and 802.11a PHY to provide network management and control extensions for spectrum and transmit power management in the 5 GHz band. This is will allow regulatory acceptance of the standard in some European countries.
 - 802.11i - Enhancing the security and authentication mechanisms of the 802.11 standard. Ongoing.
 -
 -
 -
-

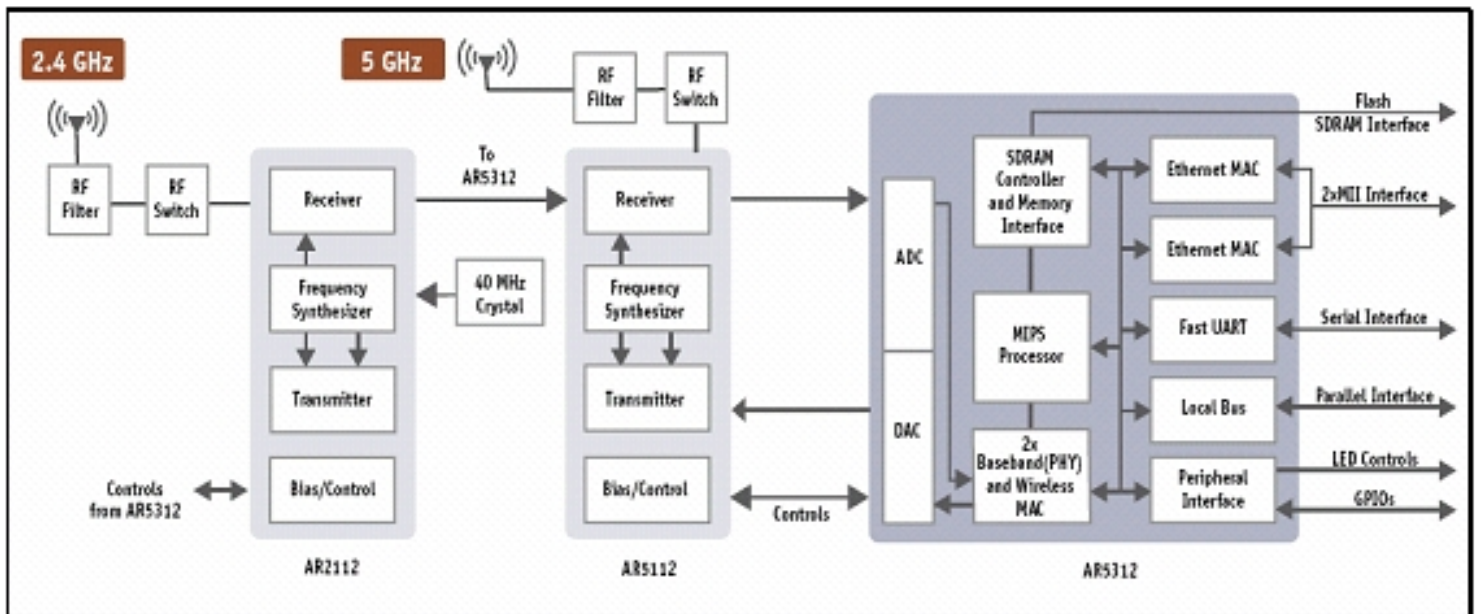
Atheros Board

Article II. Atheros Chip Set - Overview

- AR5312 System On Chip:
 - Integrated MIPS 4000 Processor
 - Supports OFDM and CCK modulation
 - Data rates of 1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, 54 Mbps and Atheros Turbo Mode offering up to 108 Mbps
 - Two IEEE 802.3 Ethernet MAC supporting 10/100 Mbps, full and half duplex, and MII interface to external Ethernet PHY
 - UART with DMA supports data rates up to 1 Mbps
 - Flexible, programmable local bus
 - EJTAG based debugging of the processor core supported
- AR 5112 & AR 2112 Radio On Chip (ROC)
 - AR5112 supports
 - f* IEEE 802.11a/b/g standards
 - f* Frequency for IEEE 802.11a 4.9 GHz to 5.85 GHz and for IEEE 802.11b/g 2.3 GHz to 2.5 GHz
 - f* Modulation Technologies OFDM with BPSK, QPSK, 16 QAM, 64 QAM DBPSK, DQPSK, CCK
 - f* Hardware Encryption WEP, AES, TKIP
 - f* Quality of service 802.1e draft
 - AR 2112 supports
 - f* IEEE 802.11b/g standards

Frequency for IEEE 802.11b/g 2.3 GHz to 2.5 GHz

- f* Modulation Technologies OFDM with BPSK, QPSK, 16 QAM, 64 QAM DBPSK, DQPSK, CCK
- f* Hardware Encryption WEP, AES, TKIP
- f* Quality of service 802.1e draft

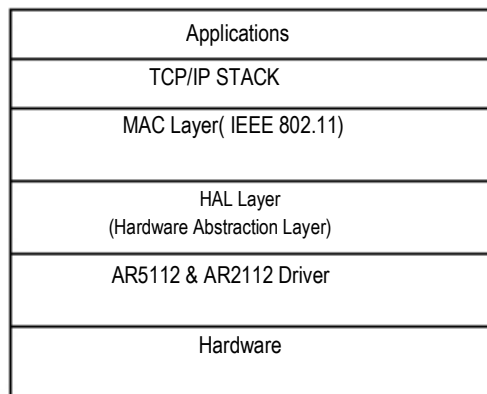


System Block Diagram

Software Developed

Article III. Driver Development

- Porting of AR5112 & AR2112 and IEEE 802.11 MAC layer drivers from VxWorks to Linux 2.4
 - Porting issues
 - f* Changing all the system calls(API) from VxWorks to Linux OS.
 - f* Converting Virtual memory to physical memory so that Radio On Chip can make DMA transfer of descriptor queues for transmission. Since VxWorks doesn't has virtual memory, in the given original VxWorks driver files its not defined
 - Following diagram shows Driver layers



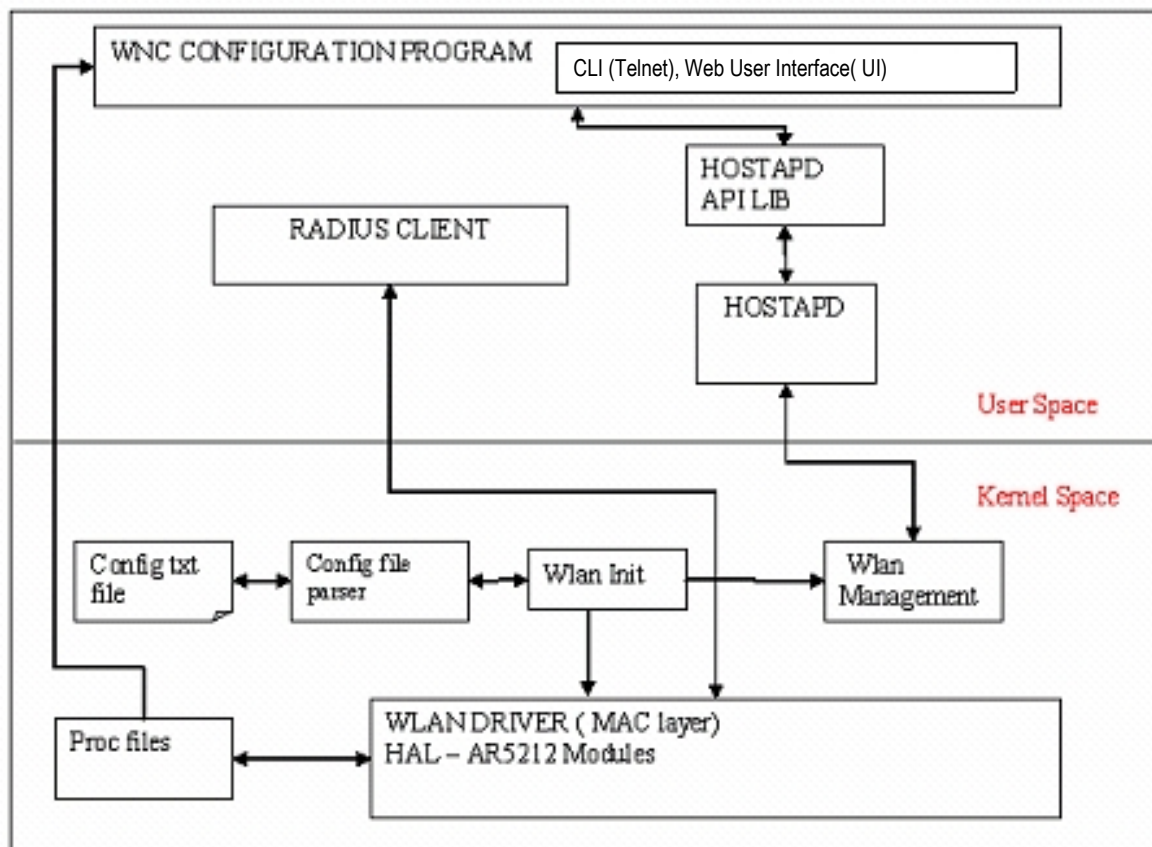
- Initialization of MAC layer
 - Initialization of Board data which includes reading MAC address of the device from EEPROM
 - Initialization of Driver data structure, Station data structure, memory allocation for transmit and receive queues
 - f* The Drivers data structure was initialized with configuration parameters read from configuration text file
 - f* The administrator of AP can modify the configuration file with following settings

- AP IP address, enabling or disabling of WEP encryption, configuring pre-shared secret key for encryption, option for 64 bit, 128bit, 154 bit keys, key type ex: hexadecimal or ASCII, configuring SSID, beacon interval, country code, Wireless mode (ex 802.11a, 802.11b or 802.11g), data rate, SSID suppress enable/disable, fragmentation threshold, software re-try enable/disable, WDS enable/disable, short preamble, RTS/CTS threshold.
 - Initialization of encryption engines for WEP, TKIP, AES
 - Registering interrupts with Linux OS & task lets i.e. bottom half
- Registering the MAC layer with Linux OS as Network Driver
 - The MAC layer is registered with Linux OS
 - The MAC layer is integrated with Linux TCP/IP stack
 - f* The MAC layer uses Atheros descriptor structure for packet transmission and receive but linux TCP/IP stack uses sk_buff structure. So there was need to convert Atheros descriptor structure to sk_buff structure and vice versa.
- Driver features
 - The " ioctl " functionality has been added to change or modify driver parameters
 - For access control MAC filtering has been added and administrator of AP can update the following files with MAC address of the stations.
 - f* MAC allow list
 - f* MAC deny list
- Log file functionality is provided with following 8 levels of messaging
 - WLAN_LOG_EMERG (High priority)
 - WLAN_LOG_ALERT
 - WLAN_LOG_CRIT
 - WLAN_LOG_ERR
 - WLAN_LOG_WARNING
 - WLAN_LOG_NOTICE
 - WLAN_LOG_INFO
 - WLAN_LOG_DEBUG (Low priority)
- Linux 'proc' files are updated with WLAN driver information

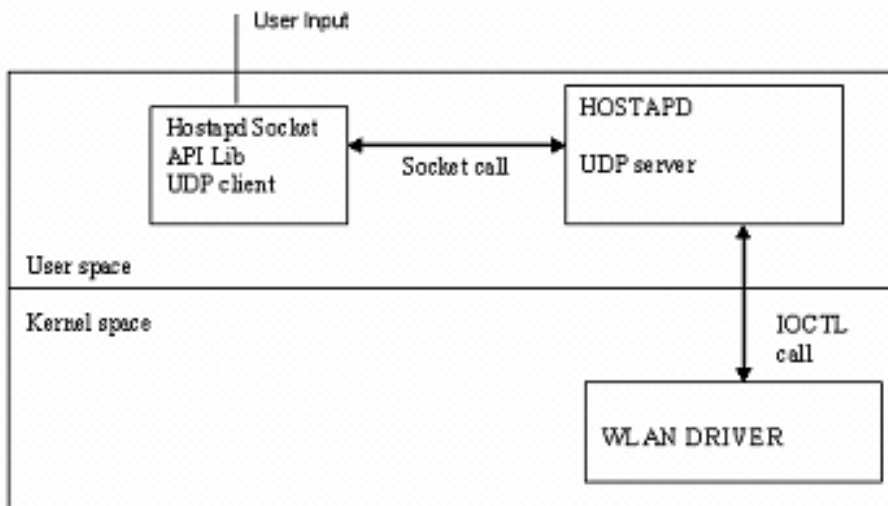
Software Developed

Article IV. Application Development

- Application module Block diagram show below
 - WNC Configuration Program: This module consists of the User Interface (UI), Web server and CLI sub-modules for managing the Wireless Access Point
 - Set of APIs are provided in to interact with HostApd module to provide service to external request from CLI(Telnet), Web UI etc...



HostApd bock diagram



- HostApd Configuration module

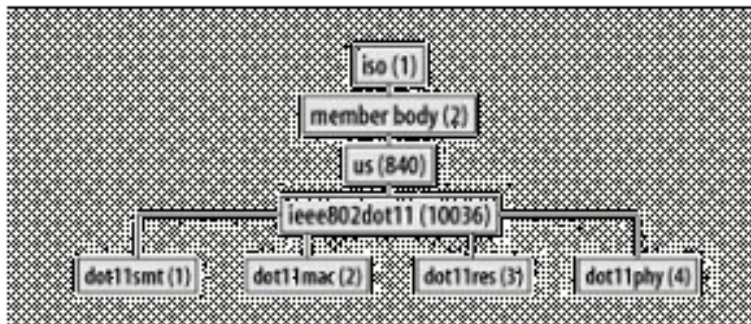
- *HostAp* Daemon module is responsible for managing the AP
- Web management, CLI and UI module interact with HostAp Daemon through APIs for various services
- The hostapd socket API Lib will open UDP socket for inter-process communication with HOSTAPD module. And HOSTAPD will communicate with WLAN Driver module which is in the kernel space through ioctl to retrieve the data from WLAN Driver.

-
- Host API module developed

- These are set of APIs developed to enable various modules to interface with AP
- API module interacts with HostApd module to deliver requested service

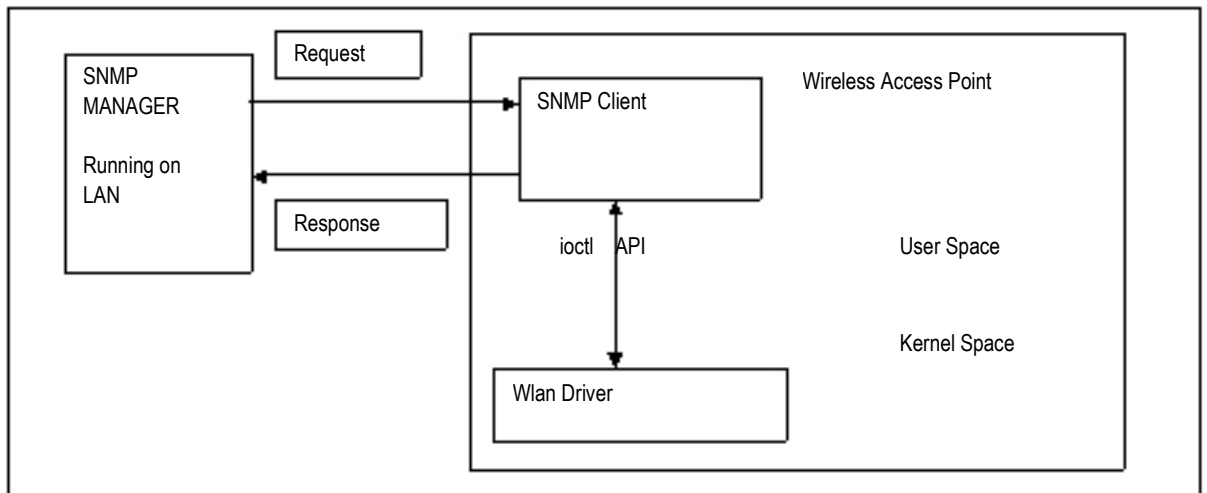
- SNMPv2(RFC 2578) client developed

- 802.11 MIB has different root: iso.member-body.us.ieee802dot11 (.1.2.840.10036)



support for following MIB variables and MIB tables are provided in the software

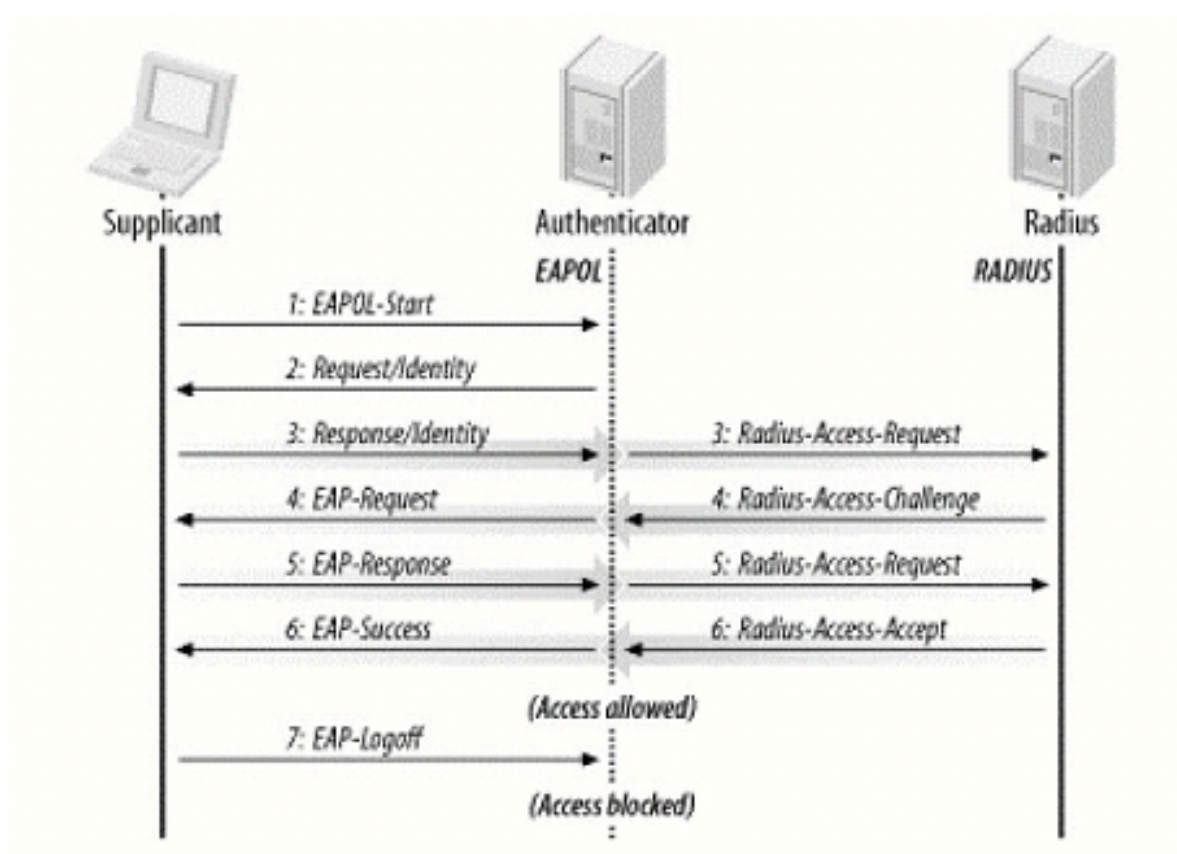
- *f* *dot11smt* Contains objects related to station management and local configuration
 - f* *dot11mac* Composed of objects that report on the status of various MAC parameters and allow configuration of them.
 - f* *dot11res* Contains objects that describe available resources
 - f* *dot11phy* Report on the status of the various physical layers
- *SNMP Block Diagram*



- f* SNMP Client is implemented in the AP.
- f* The external SNMP Manager(Manager will be running on separate PC over the network) sends requests to SNMP Client which is running on the Wireless Access Point.
- f* The requests comes from Manager in the form of ASN1(*Abstract Syntax Notation One*) notation. The SNMP Client parses the requests which is in the form of ASN notation and retrieves the data from wlan driver using Linux ioctl API.
- f* After retrieving the data from driver the SNMP Client again encodes the data in the form of ASN notation and sends back the reply message to SNMP Manager.

RADIUS client developed (EAP over RADIUS RFC 2869)

- Authentication types includes 802.1X and EAP protocols
- RADIUS Authentication & Accounting
- Primary & Backup Servers
- Fail-over limits, Re-attempt interval for the primary server
- Authentication Exchange between mobile station(Supplicant), Authenticator(AP) and Authentication Server (RADIUS) show below



* Supplicant is station(Mobile user), Authenticator is Access point, EAPOL (Extensible Authentication protocol over LAN)