# *Software Radio Interface Decomposition for Wireless Devices*

Dr. D. J. Shyy

Dawn Szelc

The MITRE Corporation

# *Agenda*

- Introduction
- IEEE 802.11
- WLAN Access Point Architecture
- "Thick" Vs "Thin" Access Point
- Standardized interfaces – OMG PIM
- Application to JTRS

MITRE

# *Introduction*

- Both the SDR Forum and the OMG are working on standards for software defined radio (SDR).
  - OMG PIM and PSM for Software Radio Components
  - Overview and Definition of Software Download for RF Reconfiguration (SDRF-02-A-0002-V0.00)
  - Requirements for Radio Software Download (SDRF-02-A-0007-V0.00)
  - Security Aspects of Operational Software Download for Commercial Wireless Devices (SDRF-02-W-0005-V0.22 Draft)
- Government and industry would both benefit from use of these standards, especially standardized interfaces, for many different wireless devices.
  - The advantages include flexibility, lower cost and portability of application software across platforms.
  - The ability for additional vendors to provide products of partial functionality.
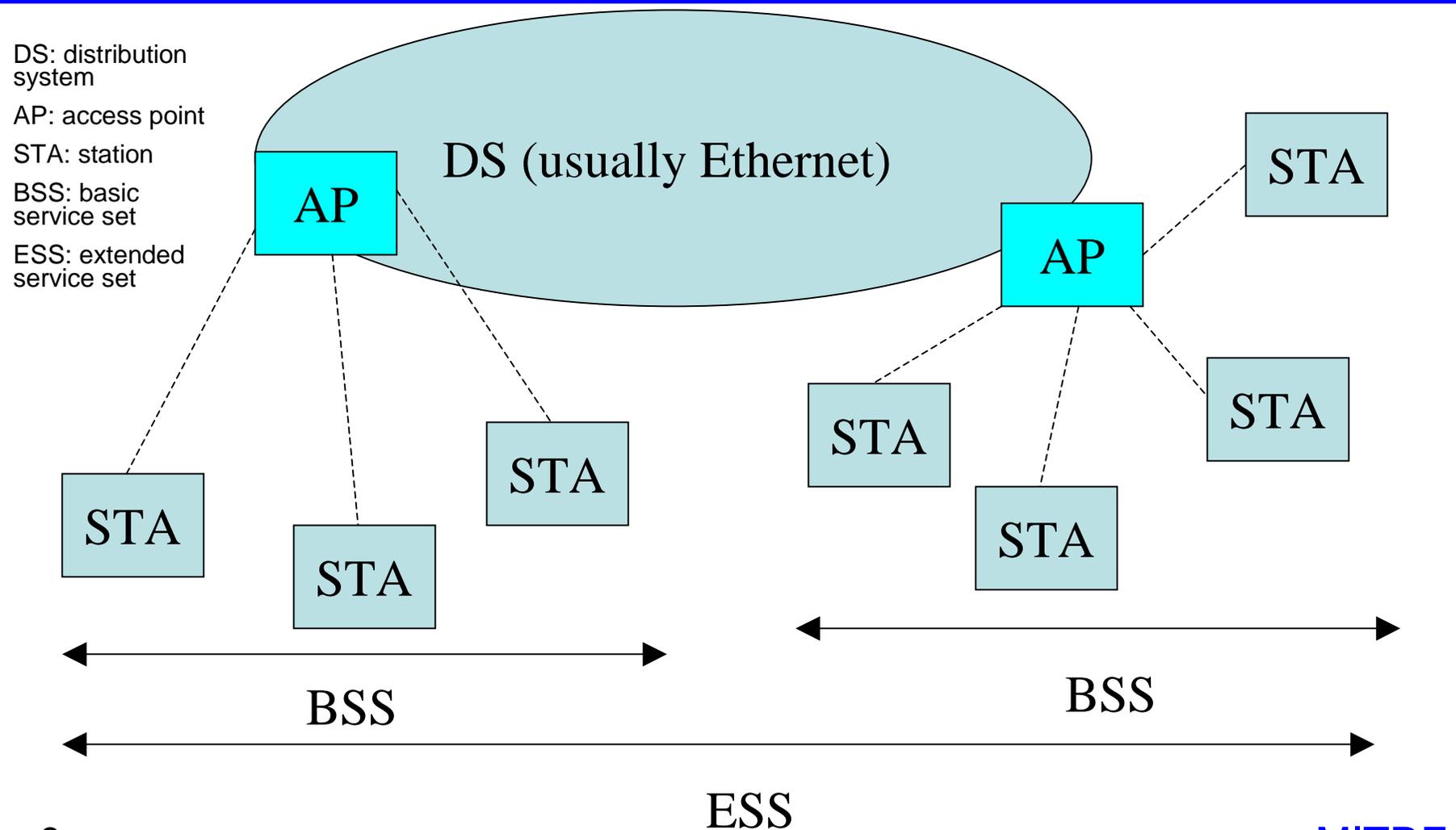- We are going to look at IEEE 802.11 WLAN as an example of how this can be accomplished.

MITRE

# *What is IEEE 802.11?*

- IEEE standard for wireless local area networks (wireless LANs)
- Developed in late 90s
- Intended for home or office use (i.e., primarily indoor)
- Standards for the MAC and PHY layers only (not for the higher layers)
- Wireless version of the Ethernet (802.3) standard

4

MITRE

# *Architecture Overview*

- One MAC supporting multiple PHYs
    - Frequency Hopping Spread Spectrum (FHSS)
    - Direct Sequence Spread Spectrum (DSSS)
    - Orthogonal Frequency Division Multiplexing (OFDM)
    - Infrared (IR)
- Two configurations
    - "infrastructure" and "independent" (ad-hoc)
- CSMA/CA (collision avoidance) with optional "point coordination"

MITRE

# *WLAN 802.11 Network*

DS: distribution system

AP: access point

STA: station

BSS: basic service set

ESS: extended service set

DS (usually Ethernet)

AP

AP

STA

STA

STA

STA

STA

STA

STA

STA

BSS

BSS

ESS

MITRE

# *Access Point and Station Relationship*

- Each node in the IEEE 802.11 network may be a STA or/and an AP

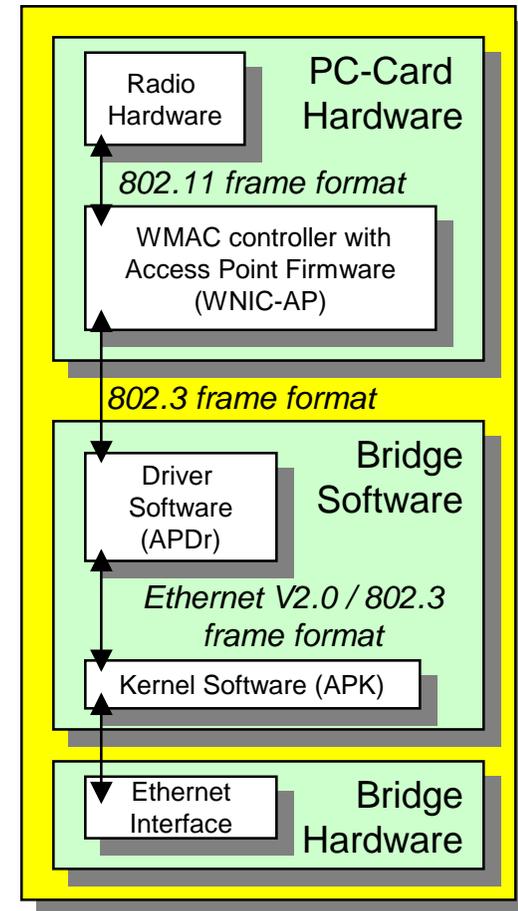- By definition, an AP contains a STA

# *Access Points*

- STAs select an AP and associate with the AP
  - Associate with the AP is the same as joining the network
- Support roaming
- Administer Point Coordination Function (PCF)
- Provide other functions
  - Time synchronization (e.g. beaconing)
  - Power management support

MITRE

# *Access Point Architecture*

- In the current WLAN implementation, an access point (AP) implements all the functionality of all the layers.
  - Costly
  - Not scalable
  - Not suitable for functions which require global view of the network
    - Resource management
    - Mobility management
    - Security management

9

# *AP Architecture (Cont'd)*

- Device that contains IEEE 802.11 conformant MAC and PHY interfaces to the wireless medium, and provides access to a distribution system for associated STAs

- Most often infrastructure products that connect to wired backbones
    - Example: implemented in Avaya Wireless IEEE 802.11 PC-Card when it is inserted in an AP-500 or AP-1000

**PC-Card Hardware**

Radio Hardware

*802.11 frame format*

WMAC controller with Access Point Firmware (WNIC-AP)

*802.3 frame format*

**Bridge Software**

Driver Software (APDr)

*Ethernet V2.0 / 802.3 frame format*

Kernel Software (APK)

**Bridge Hardware**

Ethernet Interface

10

MITRE

# *"Thin" Vs "Thick" AP*

- The current AP implementation falls into the category of "thick" AP
  - All the functions (MAC, authentication, encryption, mobility management, load balancing, IP [tunneling, routing]) are contained in each AP.

MITRE

# *"Thin" Vs "Thick" AP (Cont'd)*

- Industry is considering the use of "thin" AP for a number of reasons:
  - Reduce the amount of processing done (and cost) in the AP by moving functions suitable for centralization to a centralized controller
  - Certain functions require global network view, and their performance is not optimized with thick AP architecture
  - Easy configuration, maintenance and management of APs
  - More scalable

- "Thin" AP architecture requires the use of a centralized access controller (AC)
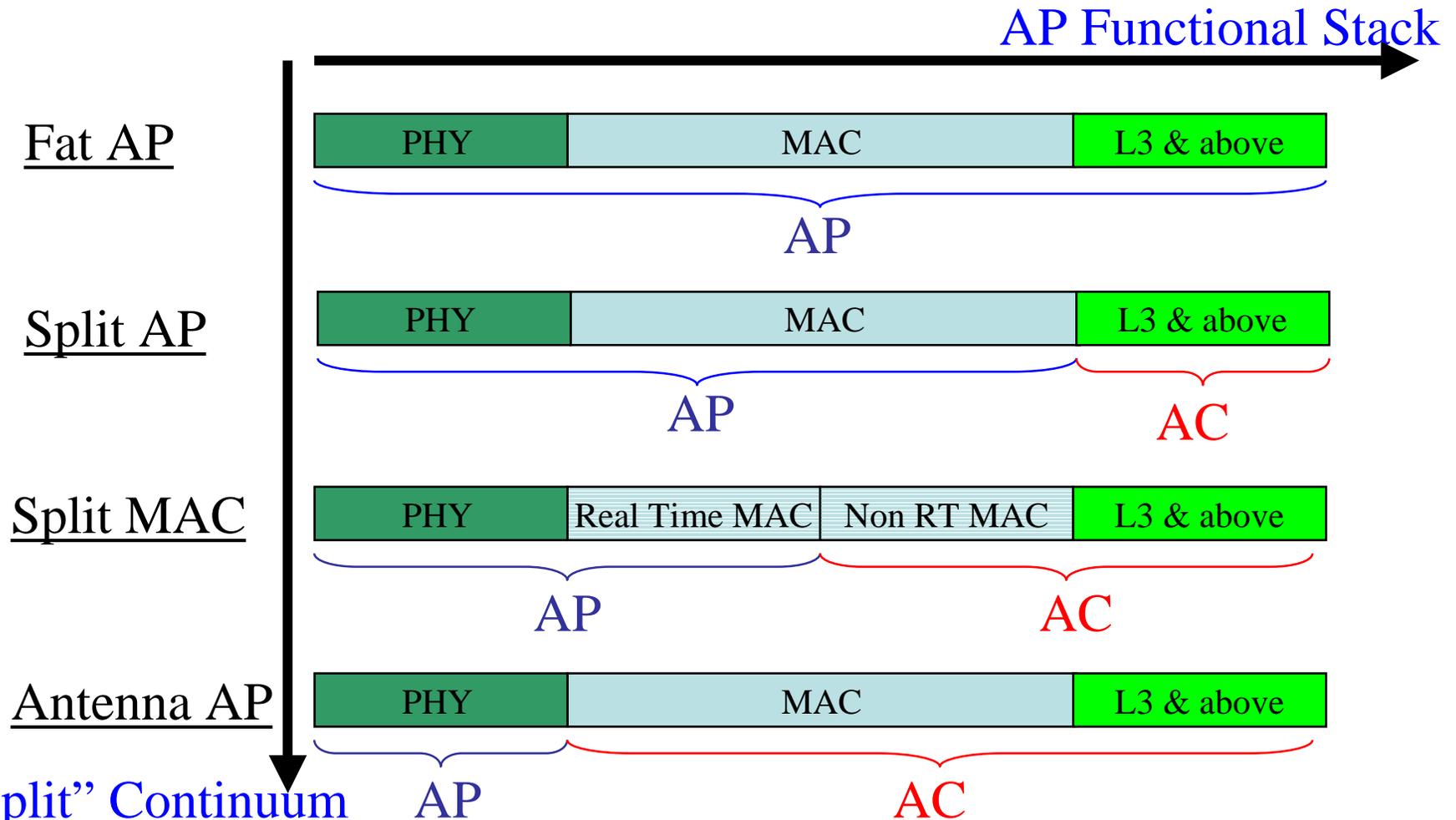  - Split of functions/layers between AP and AC is an on-going research topic

MITRE

# *Standardization Efforts in "Thin" Vs "Thick" AP*

- Both IETF Control And Provisioning of Wireless Access Points (CAPWAP) and IEEE 802.11 AP Functions Description Study Group (SG) are looking into this issue
  - Logical decomposition of AP functionality into logical units
  - Description of interfaces between these logical units

MITRE

# Split of Functions between AC and AP

- In general, <u>functions requiring global network view and unified policy</u>, <u>layers 3 and above</u>, as well as <u>non-real-time MAC</u> are good candidates to be resident in the centralized AC.  Functions that are timing-critical should be resident in AP.

- We propose to formulate a cost function considering the following factors with timing as one of the constraints:
  - RF and MAC performance (channel selection, interference mitigation)
  - Resource management (load balancing)
  - Security management
  - Mobility management (handover)

- The outcome of minimizing the cost function would be where the optimal interface is, and functions can be divided between AC and AP.

MITRE

# 802.11 "Split" Architecture Examples*

**AP Functional Stack**

| | | | |
|---|---|---|---|
| **Fat AP** | PHY | MAC | L3 & above |

AP

| | | | |
|---|---|---|---|
| **Split AP** | PHY | MAC | L3 & above |

AP     AC

| | | | | |
|---|---|---|---|---|
| **Split MAC** | PHY | Real Time MAC | Non RT MAC | L3 & above |

AP     AC

| | | | |
|---|---|---|---|
| **Antenna AP** | PHY | MAC | L3 & above |

AP     AC

"Split" Continuum

15

MITRE

# *Use of OMG standard for WLAN interfaces*

- The Software Based Communications (SBC) Domain Task Force (DTF) has recently completed the PIM for Software Radio Components

- We propose that these interface definitions be used to standardize the WLAN (or other wireless devices) interfaces for the purposes of segregating functionality between AC and AP.
  - Common Layer Facilities
  - Data Link Layer Facilities
  - Physical Layer Facilities
  - Radio Control Facilities

MITRE

# *Examples of Application of PIM to 802.11 implementations*

- **Common Layer Facilities**
  - Quality of Service is not currently implemented in 802.11 but is planned in 802.11e.  The PIM defines a QoS API (throughput, transitDelay, priority, protection, residualErrorRate, resilience) that could be used.
  - Flow Control Management API handles priorityHandling, dataRate, flowControlSignaling, and emptySignaling.  These would be mapped to the required CSMA/CA functionality from the 802.11 MAC.
  - Flow Control facilities also supply the User acknowledgement (ACK) of correctly received data units.  This maps well to the required ACK in the Distributed Coordination Function (DCF) for unicast traffic.

- **Data Link Layer Facilities**
  - Media Access Control Facilities includes some of the functions above and also handling of data and control channels, as well as scheduling of transmission, and reordering, assembly, and multiplexing of data.

MITRE

# *Thin Vs. Thick AP is Not a New Concept*

- The thin AP + AC concept follows the architecture of cellular networks, i.e., BS + BSC (which has been around for more than 20 years).

- Also, the CDMA base station vendors went through the same exercise for how to implement the soft handover feature

  - Choice I: Distributed Control - Resource allocation and admission control are done through coordination between BSs (BSC is not involved)

  - Choice II: Centralized Control - The BSC makes the sole decision

    - Due to the strict timing and synchronization requirements of CDMA soft handover, the vendor that implemented distributed soft handover scheme failed.

18

MITRE

# *Learn from the Past*

- The division of functions between cellular BS and BSC can be used as a baseline example when we perform the same task for thin AP and AC.

# *IEEE 802.11r*

- The IEEE 802.11r task group is working on techniques to speed up handover process between APs such that roaming (handover) interval can be less than 50 ms
  - The envisioned technique is make-before-break which is the technique used in CDMA soft handover
  - The thin AP + AC architecture may have advantage in controlling the handover process

MITRE

# JTRS Wireless Network Decomposition

• Current design: Each JTRS (WNW) performs as an IP router.  It has disadvantages of higher cost, larger battery, more power consumption, larger size, and more weight.
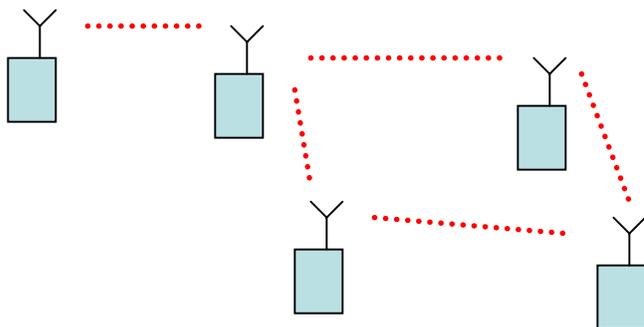


• Alternate design: Each JTRS (WNW) simply performs waveform and MAC layer functions.  The layer 3 function is placed on a centralized point of presence (POP).  All nodes are one-hop away from the POP.  The POP can be connected using SATCOM links.

MITRE

# BACKUP

MITRE
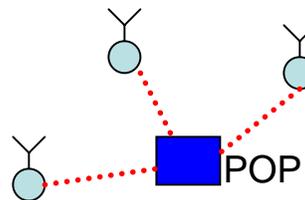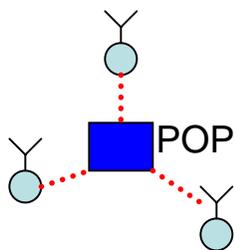
# *WLAN Global Functions*

- RF footprint (tx power)
- RF interference (channel selection)
- Load balancing
- Mobility management (handover)
- Security management (authentication)

MITRE