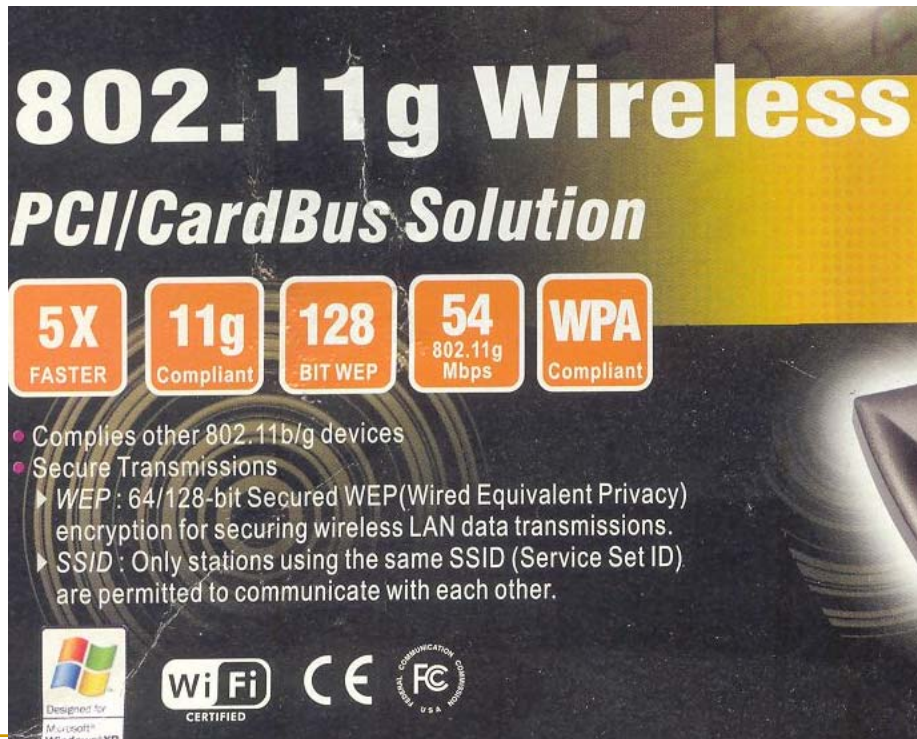


IEEE 802.11



**802.11g Wireless
PCI/CardBus Solution**

5X FASTER
11g Compliant
128 BIT WEP
54 802.11g Mbps
WPA Compliant

- Complies other 802.11b/g devices
- Secure Transmissions
 - ▶ WEP: 64/128-bit Secured WEP(Wired Equivalent Privacy) encryption for securing wireless LAN data transmissions.
 - ▶ SSID: Only stations using the same SSID (Service Set ID) are permitted to communicate with each other.

Designed for Microsoft® Windows® XP

WiFi CERTIFIED

CE

FCC COMMUNICATIONS AUTHORITY U.S.A.

Τα χαρακτηριστικά του IEEE
802.11 και οι επεκτάσεις του

Εισαγωγή

Το 802.11 και οι επεκτάσεις του:

- Επιτρέπουν την ασύρματη διασύνδεση κινούμενων ή ακίνητων συσκευών, μέσα σε μία τοπική περιοχή
 - Περιγράφουν το MAC και το PHY επίπεδο
-

Σχετικοί οργανισμοί

IEEE - Institute of Electrical and
Electronics Engineers

WECA - Wireless Ethernet Compatibility
Alliance

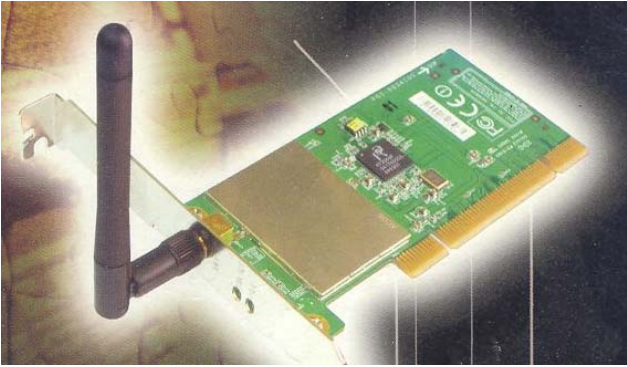
Ιστορικά στοιχεία

Το 1997 εγκρίθηκε από την ΙΕΕΕ το 802.11

Το 1999 εγκρίθηκε από την ΙΕΕΕ το 802.11b

Από τότε μέχρι σήμερα έχουν εγκριθεί είτε βρίσκονται στο στάδιο της έγκρισης μία σειρά επεκτάσεων: 802.11a,g,e,d,f,h,i

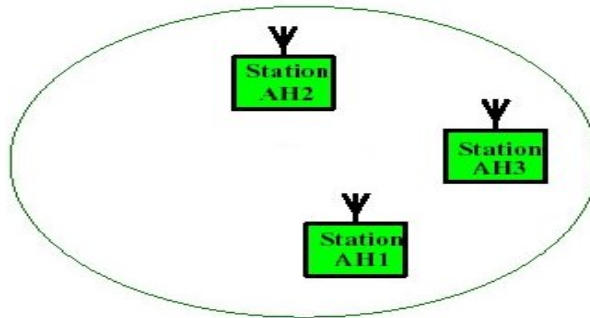




Αρχιτεκτονική του 802.11

Γενικά η αρχιτεκτονική του 802.11 μπορεί να περιγραφεί σαν ένα σύνολο από συνδεδεμένα cells

Βασικό στοιχείο της αρχιτεκτονικής είναι το Basic Service Set(BSS)



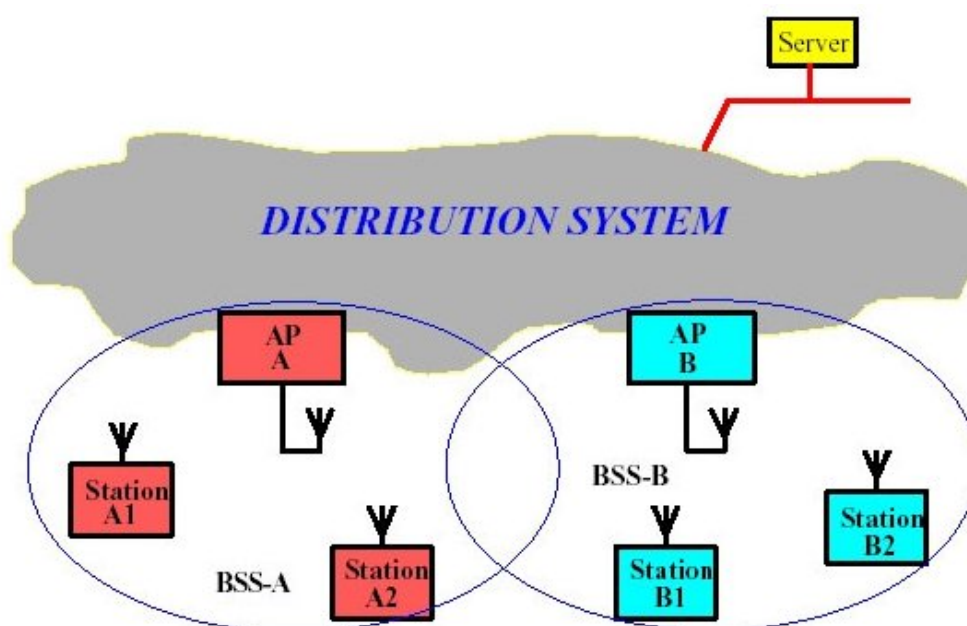
Αρχιτεκτονική του 802.11 (συνέχεια)

- Ένα BSS μπορεί να είναι αυτόνομο ή μέρος ενός μεγαλύτερου δικτύου αποτελούμενο από πολλά BSS.
 - Ένα τέτοιο δίκτυο χαρακτηρίζεται ως Extended Service Set (ESS)
 - Το Distribution System (DS) είναι το συστατικό της αρχιτεκτονικής που διασυνδέει τα BSS. Παράδειγμα DS είναι ένα ethernet LAN δίκτυο
-

Αρχιτεκτονική του 802.11 (συνέχεια)

- Η διασύνδεση ενός 802.11 δικτύου με ένα ενσύρματο δίκτυο γίνεται μέσω ενός συστατικού, γνωστού ως Access Point (AP).
- Ένα AP μπορεί ταυτόχρονα να υλοποιεί πολλά συστατικά της αρχιτεκτονικής του 802.11

Αρχιτεκτονική του 802.11 (συνέχεια)



Αρχιτεκτονική του 802.11 (συνέχεια)

Τα συστατικά της αρχιτεκτονικής θα πρέπει να προσφέρουν μία σειρά υπηρεσιών:

- Οι Station Services (SS) που παρέχονται από κάθε σταθμό:
 - authentication
 - deauthentication
 - data delivery
 - privacy
-

Αρχιτεκτονική του 802.11 (συνέχεια)

- Οι Distribution System Services (DSS) που παρέχονται από το DS:
 - association
 - reassociation
 - disassociation
 - distribution
 - integration
-

Το πρωτόκολλο - Γενικά

Το 802.11 εμφανίζεται στα ανώτερα επίπεδα (π.χ. LLC) σαν ένα ενσύρματο 802.3 δίκτυο

Το 802.11 «κρύβει» την ύπαρξη του ασύρματου μέσου καθώς και την δυνατότητα κίνησης των σταθμών

Το πρωτόκολλο – MAC

Τρία είδη πακέτων:

- Ελέγχου
- Διαχείρισης
- Δεδομένων

Ένα σημαντικός τύπος πακέτου διαχείρισης είναι το beacon

Ένας σημαντικός τύπος πακέτου ελέγχου είναι το acknowledgment

Το πρωτόκολλο – MAC (συνέχεια)

Η πρόσβαση στο κοινό μέσο καθορίζεται μέσω μίας συνάρτησης συγχρονισμού (Coordination Function - CF)

Υπάρχουν δύο ειδών CF:

- Point Coordination Function (PCF)
 - Distributed Coordination Function (DCF)
-

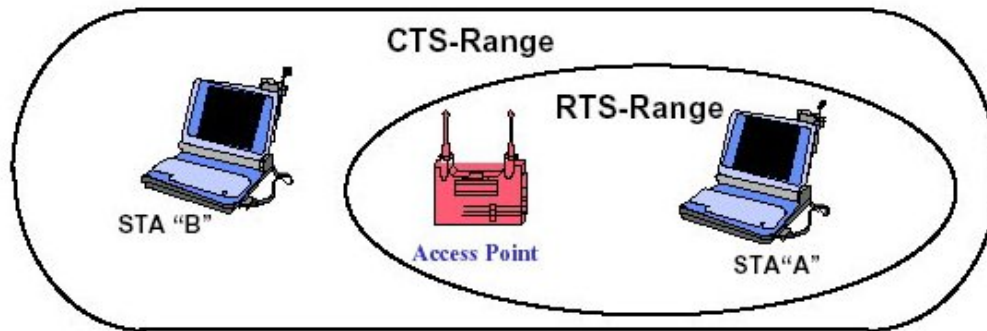
Το πρωτόκολλο – MAC (συνέχεια)

Η DCF του 802.11 είναι η Carrier Sense Multiple Access - Collision Avoidance (CSMA-CA) με binary exponential backoff

Μηχανισμός Request To Send/ Clear To Send (RTS/CTS)

Το πρωτόκολλο – MAC (συνέχεια)

Hidden terminal πρόβλημα



Το πρωτόκολλο – MAC (συνέχεια)

Το 802.11 παρέχει δύο μεθόδους για την εξασφάλιση της ασφάλειας:

- Authentication:
 - Open System
 - Shared Key
- Encryption:
 - Wired Equivalent Privacy (WEP)
 - Wi-Fi Protected Access (WPA)
 - 802.11i

Το πρωτόκολλο – MAC (συνέχεια)

Άλλα χαρακτηριστικά:

- 802.11e - Quality of Service (QoS)
 - 802.11f Inter Access Point Protocol (IAPP) – Roaming
 - 802.11h+d – Διαχείριση ισχύς και καναλιού εκπομπής
 - Power management
 - Configurable fragmentation
 - 48 bit διευθύνσεις – συμβατότητα με τα 802 πρωτόκολλα
-

Το πρωτόκολλο – PHY

Το 802.11 προσφέρει δύο επιλογές:

- infrared PHY
- radio frequency PHY

Radio frequency PHY:

- 2.4 GHz - Industrial Scientific Medical (ISM) Radio Band
 - Frequency Hopping Spread Spectrum (FHSS)
 - Direct Sequence Spread Spectrum (DSSS)
 - Μέγιστη ταχύτητα διαμεταγωγής 2Mbps
-

Το πρωτόκολλο – PHY

Το 802.11b:

- Μέγιστη ταχύτητα διαμεταγωγής 11Mbps με χρήση DSSS
- 11 κανάλια για Βόρεια Αμερική, 13 για την Ευρώπη

Το 802.11a:

- Λειτουργεί στα 5GHz
- Μέγιστη ταχύτητα διαμεταγωγής 54Mbps με χρήση Orthogonal Frequency Division Multiplexing (OFDM)
- Περισσότερα κανάλια

Το 802.11g:

- Λειτουργεί στα 2.4GHz
 - Μέγιστη ταχύτητα διαμεταγωγής 54Mbps με χρήση Orthogonal Frequency Division Multiplexing (OFDM)
-

IEEE 802.11

Η λειτουργία στην πράξη

Τα βασικά βήματα σύνδεσης

- Ο σταθμός κάνει Scan για να εντοπίσει την ύπαρξη ESS/BSS που ταιριάζει στα στοιχεία που ζητάει ο χρήστης.
 - Όταν επιλέξει το κατάλληλο BSS ξεκινάει τη διαδικασία του Authentication
 - Μετά την επιτυχή ολοκλήρωση του Authentication, ο σταθμός ξεκινάει τη διαδικασία του Association
 - Αφού τελειώσει και το Association με επιτυχία, ο σταθμός μπορεί να προχωρήσει στην ανταλλαγή δεδομένων με το δίκτυο
-

Εντοπισμός των BSS και ESS

- Η διαδικασία λέγεται *scanning*, και μπορεί να γίνει με δύο τρόπους:
 - **Passive scanning:** Ο σταθμός «αφουγκράζεται» **μόνο** τα Beacons που εκπέμπονται από τα BSSs.
 - **Active scanning:** Ο σταθμός εκτός του να αφουγκράζεται τα Beacons, εκπέμπει σε κάθε κανάλι ειδικά πακέτα τα οποία λέγονται Probe Requests, και στα οποία πρέπει να απαντάνε όλα τα BSS των οποίων τα χαρακτηριστικά ταιριάζουν με αυτά που ζητούνται στο Probe request.
-

Διαδικασία Authentication (Open System)

- Ο σταθμός στέλνει στο AP ένα authentication request
 - Το AP απαντάει με ένα πακέτο authentication response
-

Διαδικασία Authentication (Shared Key)

- Ο σταθμός στέλνει στο AP ένα authentication request
 - Το AP απαντάει με ένα πακέτο authentication challenge response, το οποίο περιέχει ένα challenge text, το οποίο είναι encrypted με τα κλειδιά που πρέπει από πριν να τα ξέρουν τόσο το AP όσο και ο σταθμός.
 - Ο σταθμός κάνει decrypt το challenge text, το ξανακάνει encrypt και το κάνει το στέλνει πίσω στο AP με ένα authentication challenge text.
 - Το AP κάνει decrypt το challenge text και το συγκρίνει με αυτό που είχε στείλει στο σταθμό. Στη συνέχεια στέλνει authentication response στο σταθμό με το κατάλληλο κωδικό αποτελέσματος.
-

Πιθανές απαντήσεις του AP σε Authentication Request

- Success
 - Authentication algorithm not supported
 - Authentication transaction sequence number error
 - Authentication reject timeout
 - Authentication reject challenge
 - Unspecified
-

Διαδικασία Association

- Ο σταθμός στέλνει στο AP ένα association request
 - Το AP απαντάει με ένα πακέτο association response
-

Πιθανές απαντήσεις του AP σε Association Request

- Success
 - Association denied
 - Support Capabilities Error
 - Denied Handle AP
 - Denied BSS Rate
 - Algorithm not supported
 - Unspecified
-

IEEE 802.11

Η αρχιτεκτονική
μιας 802.11 συμβατής συσκευής

Βασικά είδη 802.11 συσκευών

- **Station (STA):** Τερματική συσκευή προοριζόμενη για client. Μπορεί να θεωρηθεί αντίστοιχη του Ethernet NIC των Wired Networks.
 - **Access Point (AP):** Συσκευή παροχής Wireless και Network υπηρεσιών. Μπορεί να θεωρηθεί αντίστοιχη ενός Router ή ενός Switch των Wired Networks
-

Station (STA)

- Ως station συσκευή μπορεί να θεωρηθεί οποιαδήποτε συσκευή η οποία έχει ένα τουλάχιστο MAC (Medium Access Control) συμβατό με το standard IEEE 802.11, και ένα physical layer (PHY) interface στο ασύρματο μέσο μετάδοσης (wireless medium-WM), όπως ορίζεται από το standard.
 - Από την πλευρά του Host «φαίνεται» όπως και μια οποιαδήποτε άλλη κάρτα δικτύου, με τη μόνη διαφορά ότι χρειάζεται και η χρήση ειδικού λογισμικού ελέγχου της που παρέχεται από τον κατασκευαστή.
-

Access Point (AP)

- Ως Access Point (AP) μπορεί να χαρακτηριστεί οποιαδήποτε συσκευή η οποία έχει ότι και ένα **Station**, και επιπλέον παρέχει υπηρεσίες πρόσβασης στο ασύρματο και ενσύρματο δίκτυο στο οποίο ανήκει, καθώς και στις υπηρεσίες διανέμονται στα τερματικά του δικτύου, δια του ασύρματου μέσου (WM) στις συνδεδεμένες (associated) με αυτό ασύρματες συσκευές.
 - Από την πλευρά του Wired Network, «φαίνεται» το ίδιο με οποιαδήποτε άλλη συσκευή, και μπορεί να παρέχει δικτυακές υπηρεσίες όπως DHCP server, Routing μεταξύ Wired και Wireless τερματικών, SNMP services, Web, ftp, κ.ά.
-

Κύρια μέρη μιας 802.11 συσκευής (1/3)

- MAC
 - Λειτουργίες συντονισμού ενεργειών για να γίνει η μετάδοση.
 - Λειτουργίες DCF & PCF με CSMA/CA
 - Διαχείριση frames τύπου Management (Association, Authentication), Control (RTS/CTS/ACK) και Data
 - Συγχρονισμός του ασύρματου δικτύου μέσω των Beacon frames
 - Λειτουργίες κρυπτογράφησης των δεδομένων με τη χρήση καλώς ορισμένων αλγορίθμων (WEP, TKIP, AES,...)
-

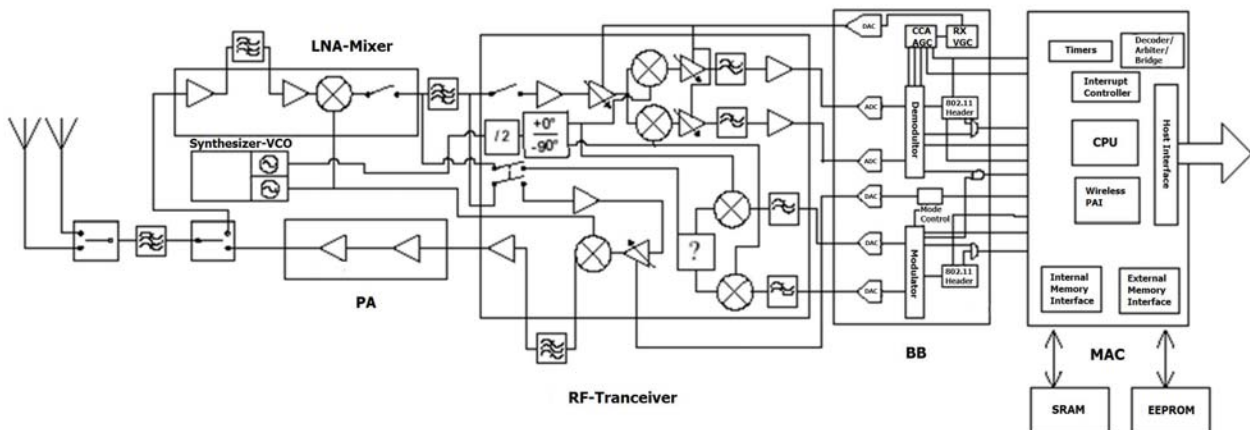
Κύρια μέρη μιας 802.11 συσκευής (2/3)

- ❑ Δυνατότητα Fragmentation & reassembly των Data frames
 - ❑ Μηχανισμοί διαχείρισης της ενέργειας (Power Save) για τη μείωση της κατανάλωσης
 - ❑ Υποστήριξη τουλάχιστον ενός Interface για τη διασύνδεσή της 802.11 συσκευής με το Host. Τυπικά παραδείγματα υποστηριζόμενων interfaces για συσκευές τύπου station είναι: PCMCIA, PCI/MiniPCI, Compact Flash, USB 1.1/2.0, ενώ για συσκευές τύπου AP: 10/100 Mbps Ethernet, SPI, ADSL.
-

Κύρια μέρη μιας 802.11 συσκευής (3/2)

- PHY
 - ❑ Baseband
 - Διεκπεραιώνει τη διαμόρφωση / αποδιαμόρφωση των εξερχόμενων / εισερχόμενων frames
 - Παράγει τα κατάλληλα αναλογικά σήματα ελέγχου του radio
 - Προσθέτει τις κατάλληλες ακολουθίες προπορευόμενων bits για την επίτευξη συγχρονισμού transmitter / receiver
 - Παράγει τα κατάλληλα σήματα που χρησιμοποιούνται στη λήψη αποφάσεων από το MAC σχετικά με τη χρήση του WM
 - ❑ Radio
 - Transceiver
 - Power Amplifier
 - LNA-Mixer
 - Synthesizer/VCO
-

Διάγραμμα μιας 802.11 συσκευής



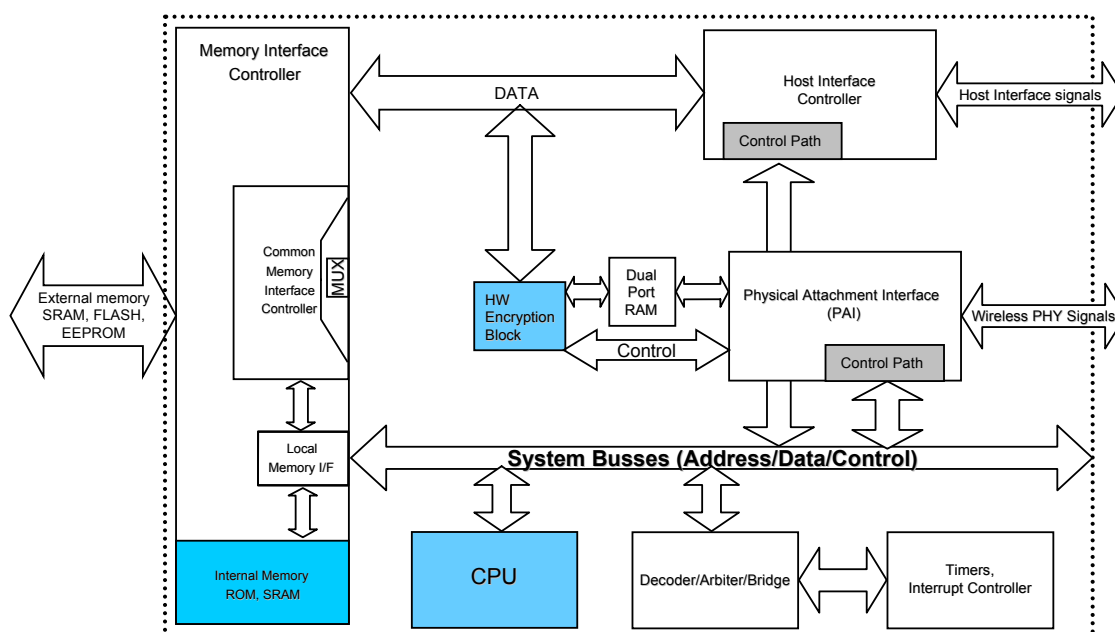
Δομικά στοιχεία του MAC (1/2)

- **Memory και Memory Interface Controller**
 - **External Memory Interface.** Είναι απαραίτητο τόσο για την επεκτασιμότητα του συστήματος όσο και για την δυνατότητα υποστήριξης υλοποιήσεων ειδικού σκοπού.
 - Είναι επιθυμητό να έχει ενσωματωμένη **SRAM**, ώστε η εκτέλεση του κώδικα και η αποθήκευση των πλέον συχνά χρησιμοποιούμενων δεδομένων να γίνεται από εκεί. Αυτό προσφέρει ταχύτητα και εξοικονόμηση ενέργειας
 - Είναι χρήσιμο να υποστηρίξει **Flash Memory Interface**, για την αποθήκευση σε **Non-volatile Memory** του κώδικα του προγράμματος. Αυτό είναι χρήσιμο όταν η συσκευή είτε απευθύνεται στη χρήση σε περιβάλλοντα που δεν μπορούν να παρέχουν τον κώδικα κατά την εκκίνηση, είτε λόγω χρονικών περιορισμών που εγείρει ο **Host** σχετικά με το **Boot Time** μιας συσκευής, είτε ακόμα γιατί έχουμε να κάνουμε με μια αυτόνομη (**Stand-Alone**) συσκευή όπως ένα **AP**.

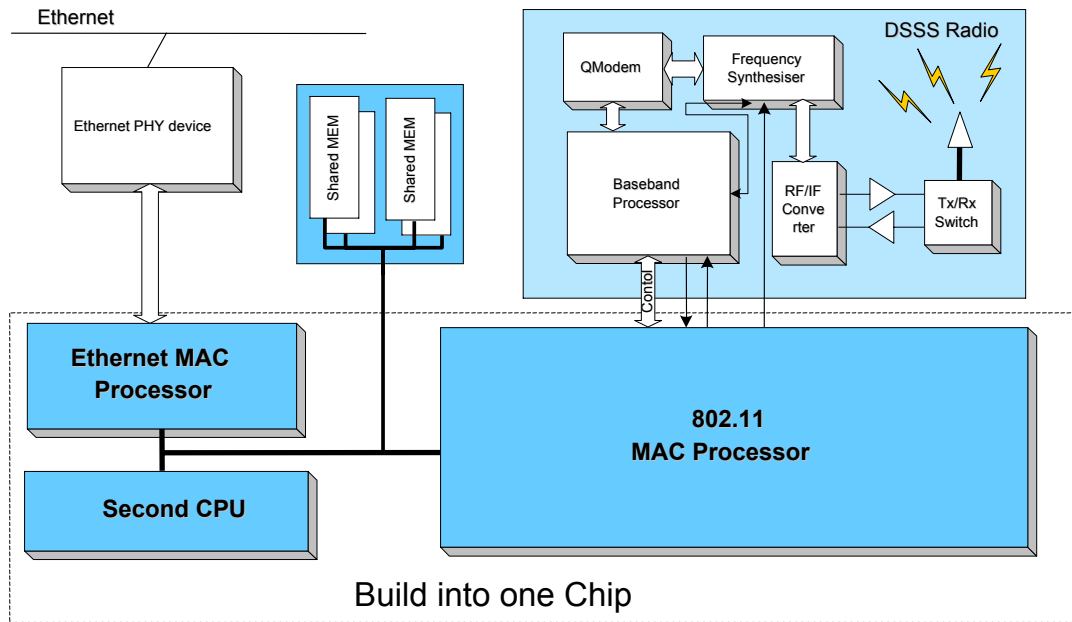
Δομικά στοιχεία του MAC (2/2)

- HW Encryption Block
 - Παρέχει τη δυνατότητα Enciphering/Deciphering των Data On-the-fly για την εξασφάλιση της προστασίας των δεδομένων
- Integrated Physical Attachment Interface (PAI)
 - Υποστηρίζει πλήρως το Direct-sequence Spread Spectrum και το Frequency-hopping Spread Spectrum Physical-layer Interfaces.
- Επιθυμητά πρόσθετα χαρακτηριστικά
 - SPI interface. Πολύ χρήσιμο για την επικοινωνία με Serial Flash ή και με BB ο οποίος δεν είναι συμβατός με το υπάρχον interface διασύνδεσης
 - GPIO pins. Τα γενικού σκοπού I/O pins μπορούν να χρησιμοποιηθούν με πολλούς τρόπους, όπως για παράδειγμα στην επέκταση της συσκευής ώστε να παρέχει και άλλες υπηρεσίες (π.χ. Mass storage)

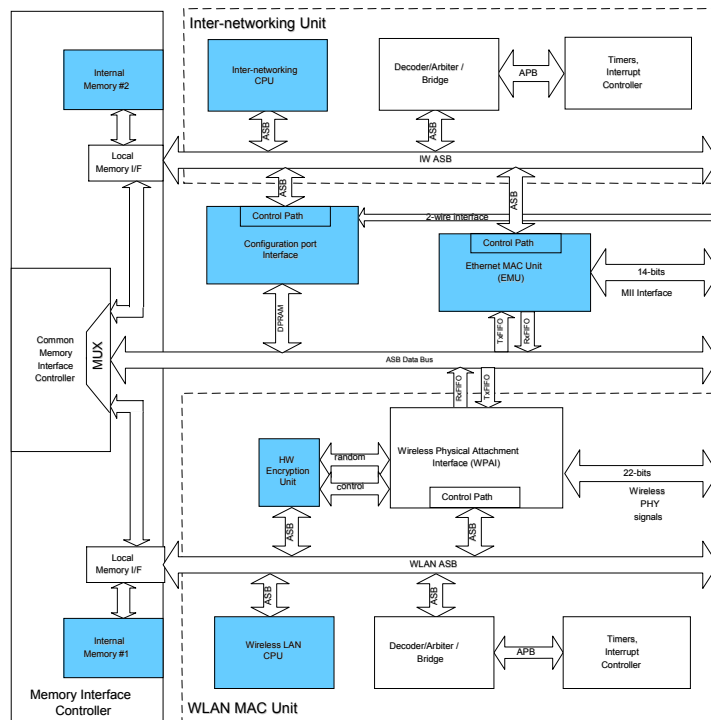
Διάγραμμα ενός 802.11 MAC



Τυπικό διάγραμμα ενός AP



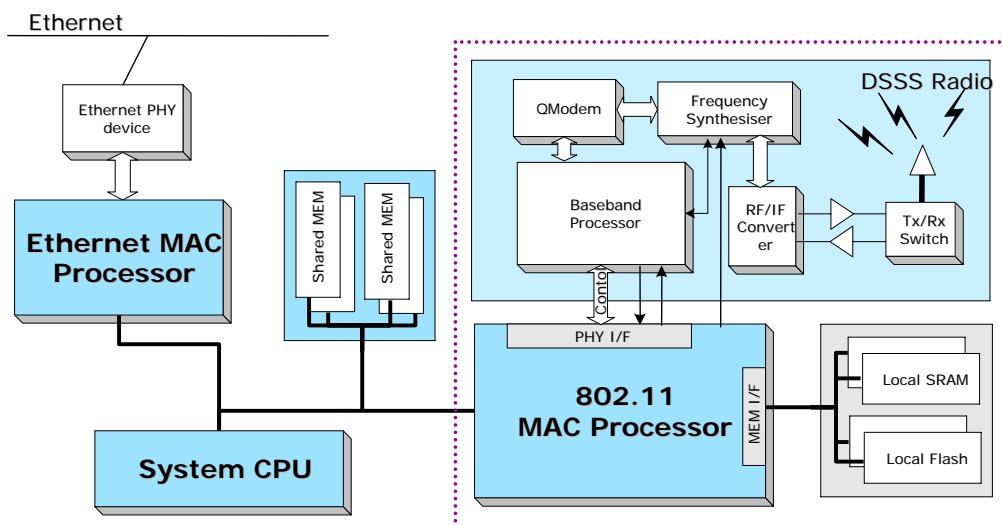
Block διάγραμμα ενός multi-CPU AP chip



Software AP βασισμένο σε station

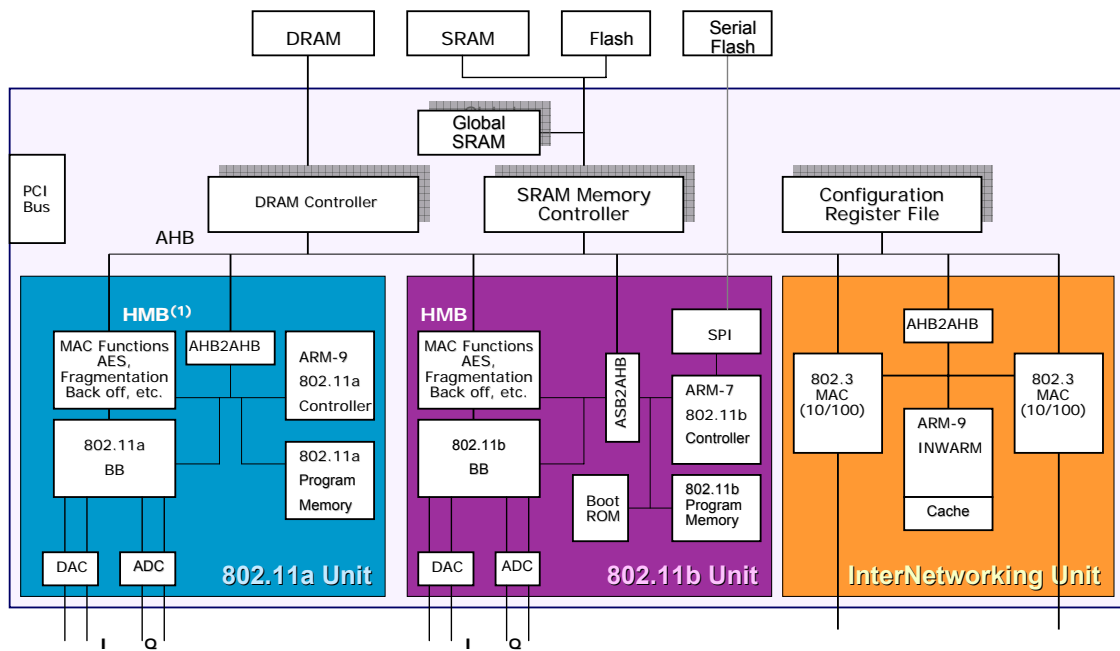
- Τα STA και τα AP έχουν το ίδιο MAC και PHY.
- Τα STA και AP διαφέρουν στα ακόλουθα:
 - Παρεχόμενες υπηρεσίες
 - Αυτονομία λειτουργίας
- Τα STA με κατάλληλο SW στο 802.11 device, και στο Host, μπορούν να παρέχουν όλες τις υπηρεσίες ενός AP, αλλά δεν θα είναι το ίδιο αυτόνομα. Οι λύσεις αυτές λέγονται Software APs
- Ο λόγος ύπαρξής τους είναι η εύκολη και φθηνή αλλαγή χρήσης και τρόπου λειτουργία μια συσκευής (πχ set-top-boxes)

Αρχιτεκτονική του SW-AP



Το μέλλον έρχεται ...

με «multi-mode/multi CPU» (1/2)



Το μέλλον έρχεται ...

με «multi-mode/multi CPU» (2/2)

