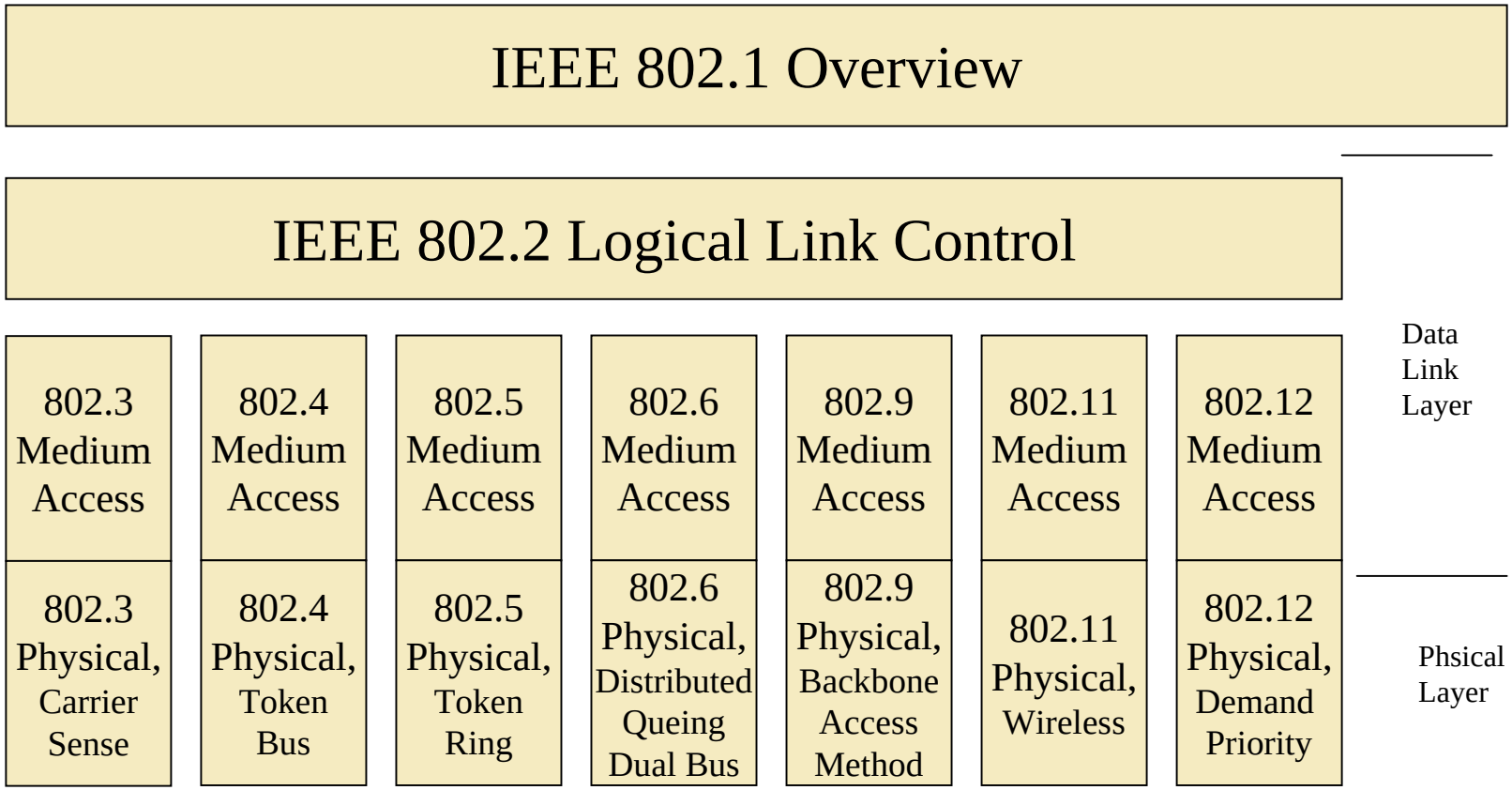
Overview of 802.11 Networks and Standards

Mauri Kangas, Helsinki University of Technology, 17.02.2004

Family of 802.xx Standards

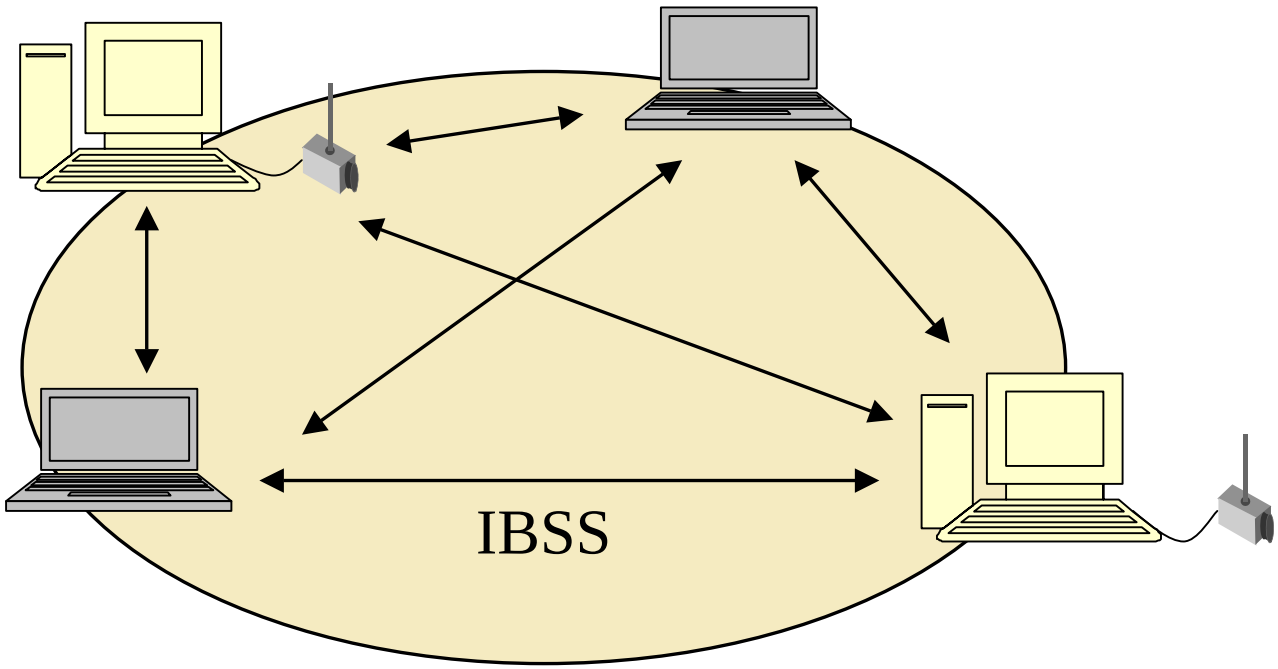
ISO/IEC 8802-xx = IEEE 802.xx



Features of the standard IEEE 802.11

- Describes the functions, services and mobility aspects required by an IEEE 802.11 device to operate within ad hoc and infrastructure networks.
- Defines the MAC procedures to support the asynchronous MAC service data unit (MSDU) delivery services.
- Defines several PHY signaling techniques and interface functions that are controlled by the IEEE 802.11 MAC.
- Permits the operation of an IEEE 802.11 conformant device within a wireless local area network (LAN) that may coexist with multiple overlapping IEEE 802.11 wireless LANs.
- Describes the requirements and procedures to provide privacy of user information being transferred over the wireless medium (WM) and authentication of IEEE 802.11 conformant devices.

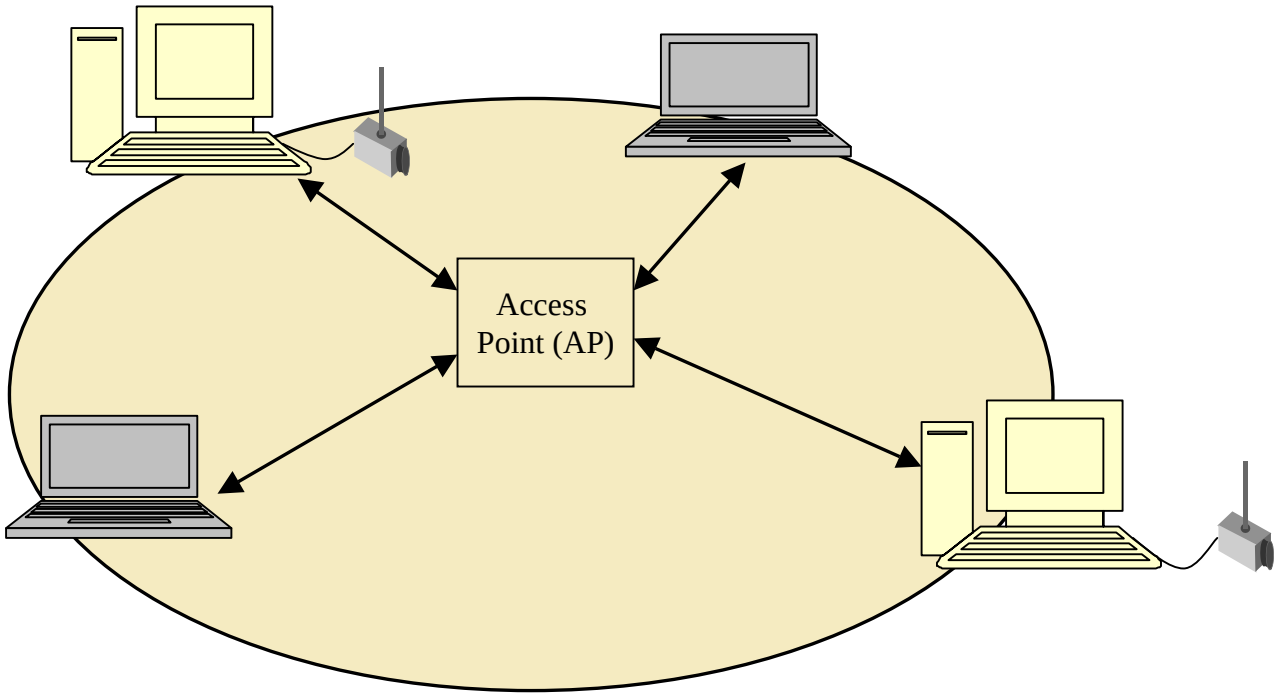
Independent Basic Service Set (IBSS)



Independent Basic Service Set (IBSS)

- A Basic Service Set (BSS) which forms a self-contained network in which no access to a Distribution System is available
- A BSS without an Access-Point
- One of the stations in the IBSS can be configured to “initiate” the network and assume the Coordination Function
- Diameter of the cell determined by coverage distance between two wireless stations

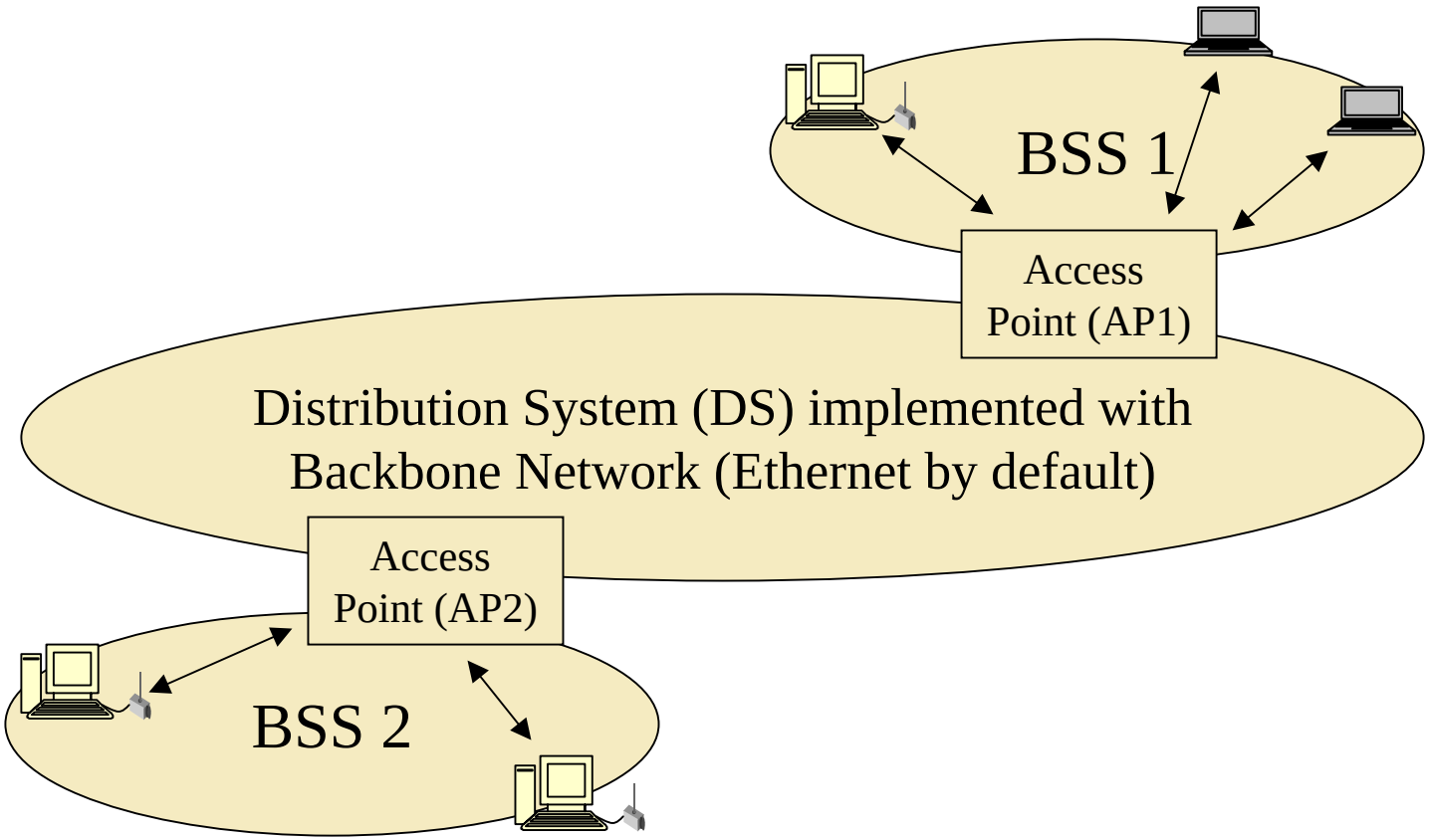
Infrastructure BSS



Infrastructure BSS Features

- All mobile stations must be accessible by the access point of the infrastructure BSS, but no restriction is placed on the distance between mobile stations themselves
- Access points in infrastructure networks can assist stations to save power
- In the infrastructure network, stations must associate with the access point in order to get access to network services
  - Mobile stations initiate the association process
  - Access points may grant or deny the access

Extended Service Set (ESS) Networks



Extended Service Set (ESS) Networks

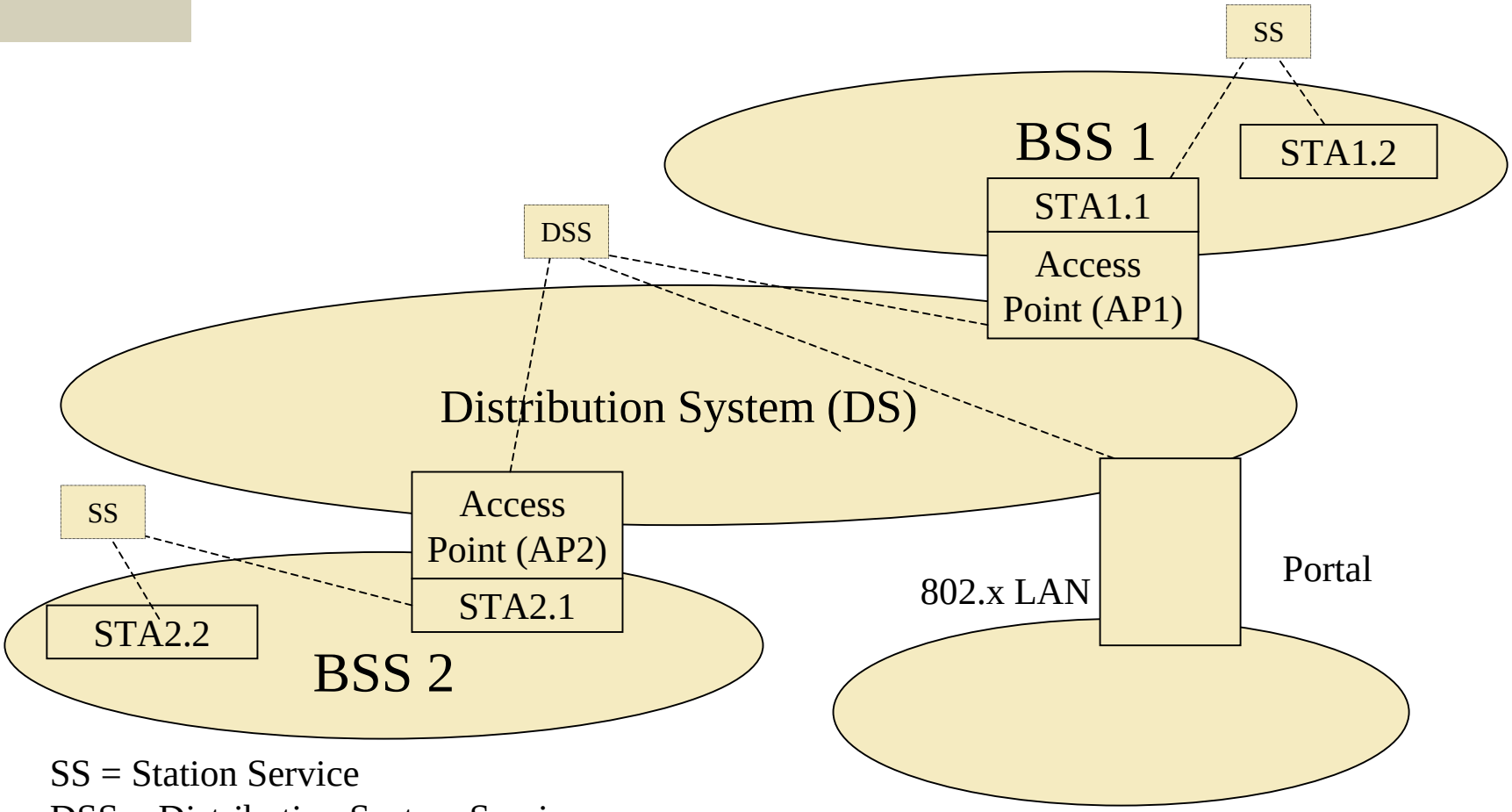
Extended Service Set (ESS):

- A set of one or more Basic Service Sets interconnected by a Distribution System (DS)
- Traffic always flows via Access-Point
- Diameter of the cell is double the coverage distance between two wireless stations

Distribution System (DS):

- A system to interconnect a set of Basic Service Sets
  - Integrated; A single Access-Point in a standalone network
  - Wired; Using cable to interconnect the Access-Points
  - Wireless; Using wireless to interconnect the Access-Points

Networking with Wired and Wireless IEEE 802 LANs



SS = Station Service
DSS = Distribution System Service

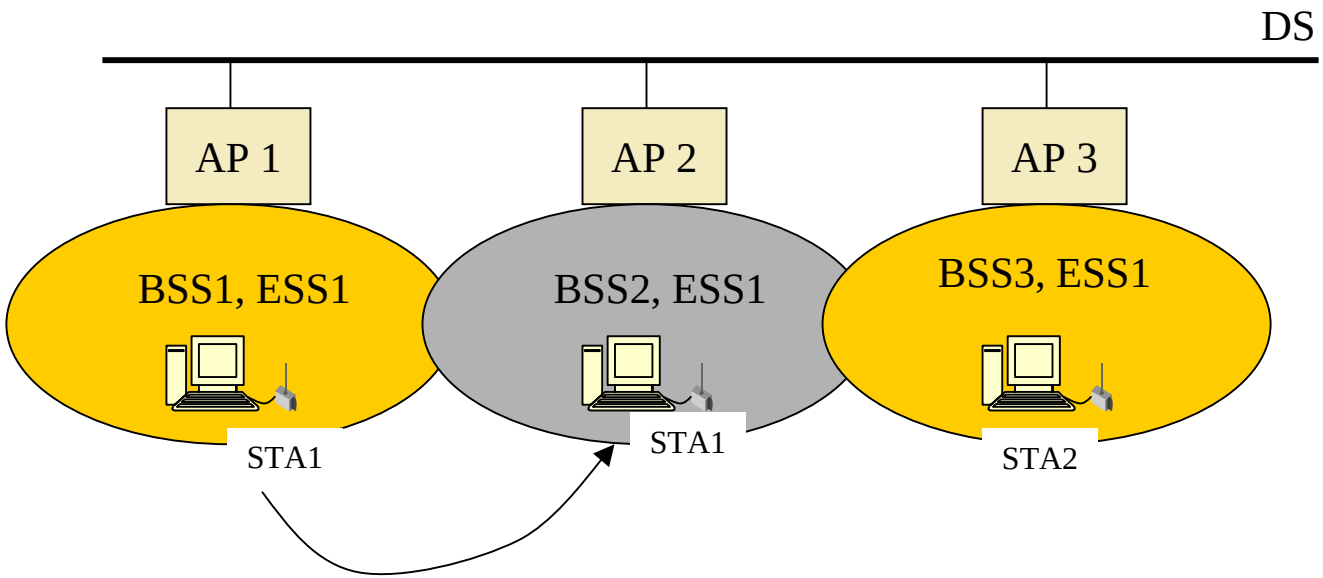
Station Services

- Authentication
  - Open System Authentication
    - Sender sends auth-msg with sender-ID , response=OK, if identity OK
  - Shared key Authentication
    - Both stations have shared secret and authentication using shared secret keys
- Deauthentication
  - Just notification will be sent to the receiver, and it cannot be refused
- Privacy
  - 802.11 Wired Equivalent Privacy (WEP) algorithm is used

Distribution System Services

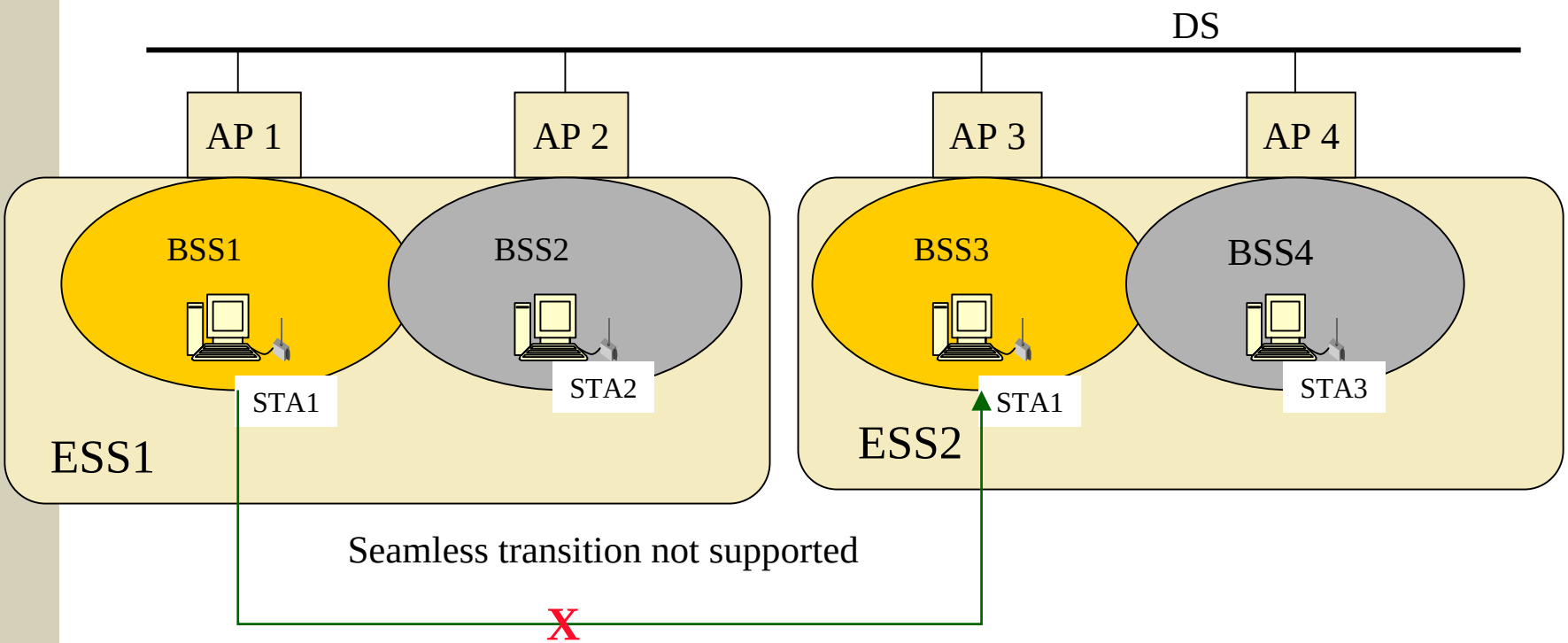
- Association
  - Each station must initially invoke the *association service* with an access point
  - The association maps a station to the distribution system via an access point
- Disassociation (= termination of an association)
- Distribution
  - Access point uses the *distribution service* every time it sends MAC frames across a distribution system
- Integration
  - The *integration service* enables the delivery of MAC frames through a portal between distribution system and a non-802.11 LAN
- Reassociation
  - The *reassociation service* enables a station to transition its association from one access point to another

Mobility Support - BSS Transition



- Station STA1 uses re-association service when moving from BSS1 to BSS2
- BSS transitions require co-operation between AP1 and AP2
- 802.11 standard doesn't specify in detail the communications what happen between AP1 and AP2 during the re-association process

Mobility Support - ESS Transition



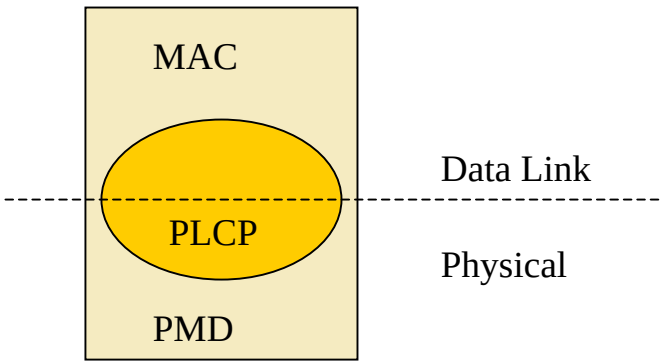
- IEEE 802.11 doesn't support ESS transition
- IEEE 802.11 just allows station (STA1) to associate AP3 in BSS3 in the second ESS (ESS2, when it has first left the first ESS (ESS1)

IEEE 802.11 Physical Layer

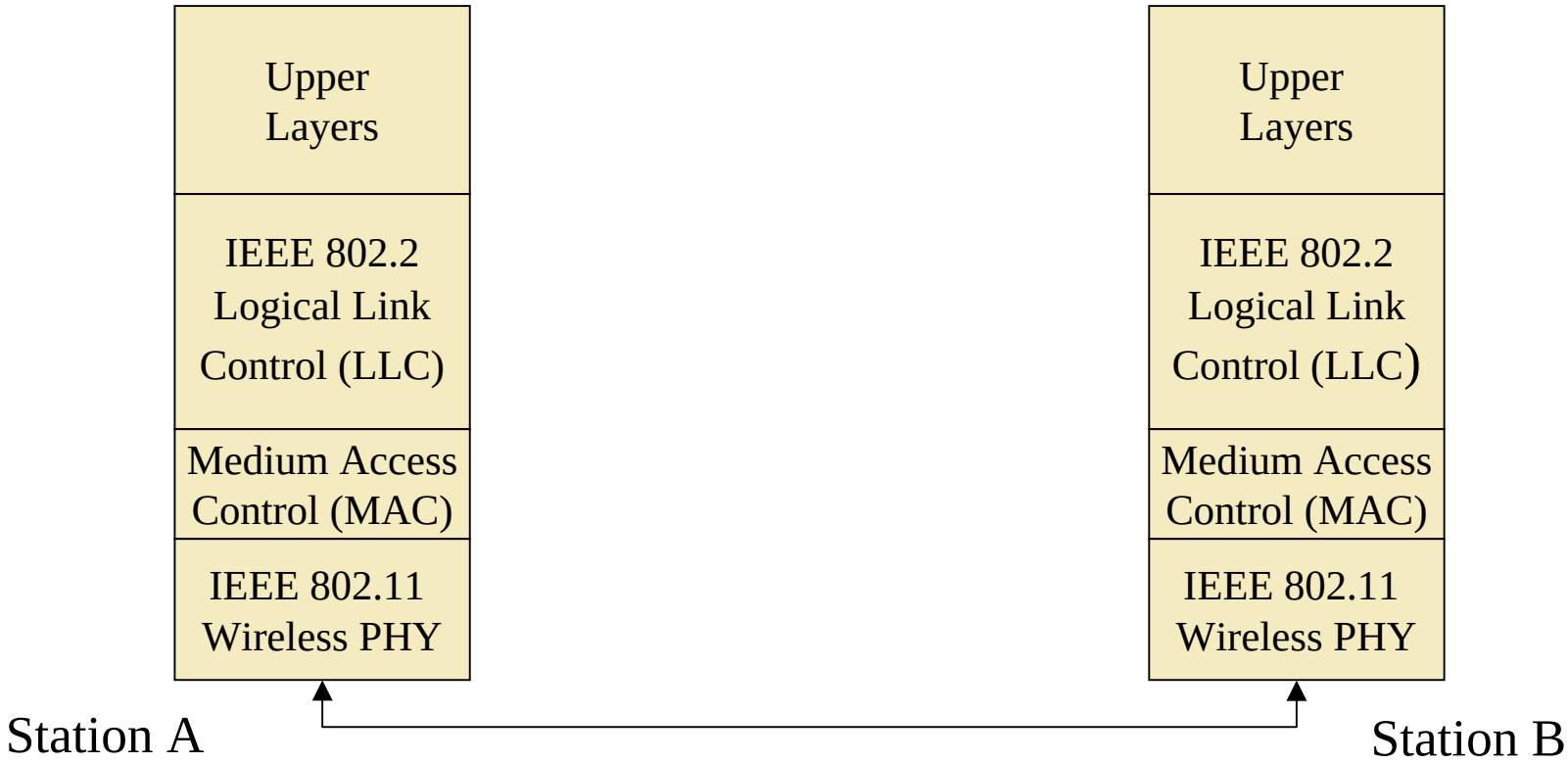
- IEEE 802.11 contains three different physical layer implementations:
  1. FHSS = Frequency Hopping Spread Spectrum
     - 2.4 GHz (2.4000-2.4835 GHz) band
     - In U.S. a maximum of 79 channels are specified in the hopping set:
       - » First ch = 2.402 GHz, others spaced by 1 MHz
       - » Channel separation corresponds to 1 Mbps instantaneous bandwidth
     - The basic 1 Mbps rate uses two-level Gaussian Frequency Shift Keying (GFSK)
  2. DSSS = Direct Sequence Spread Spectrum
     - 2.4 GHz (2.4000-2.4835 GHz) band
     - Data rates of 1 Mbps and/or 2 Mbps
       - » Basic rate of 1 Mbps is encoded using Differential Binary Phase Shift Keying (DBPSK)
       - » Enhanced 2 Mbps data rate uses differential Quadrature Phase Shift Keying (DQPSK)
     - Overlapping and adjacent BSSs can be accommodated by ensuring that the center frequencies of each BSS are separated by at least 30 MHz.
  3. IR = InfraRed
     - Wavelength range from 850 to 950 nm
     - 1 Mbps with 16-Pulse Position Modulation (16-PPM) with 4 bits mapped into 16 bits and 2 Mbps is using 4-PPM with 2 bits mapped to 4 coded bits in transmission

Physical (PHY) Layer Components

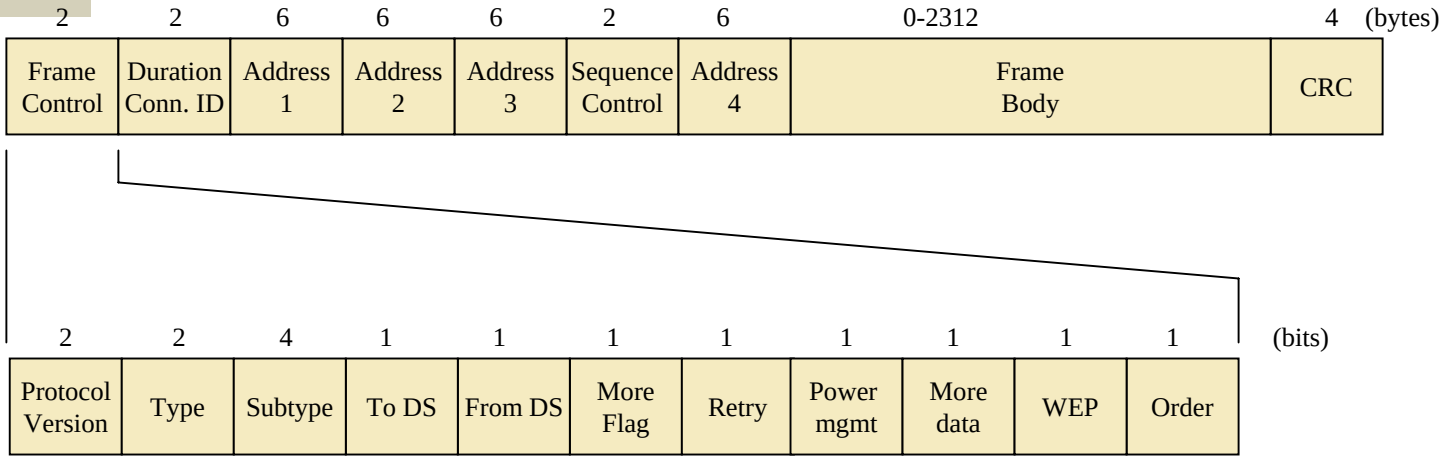
- 802.11 splits the PHY into two generic components:
  - The Physical Layer Convergence Procedure (PLCP) to map the MAC frames onto the medium
  - The Physical Medium Dependent (PMD) system to transmit those frames



IEEE 802.11 Protocol Stack



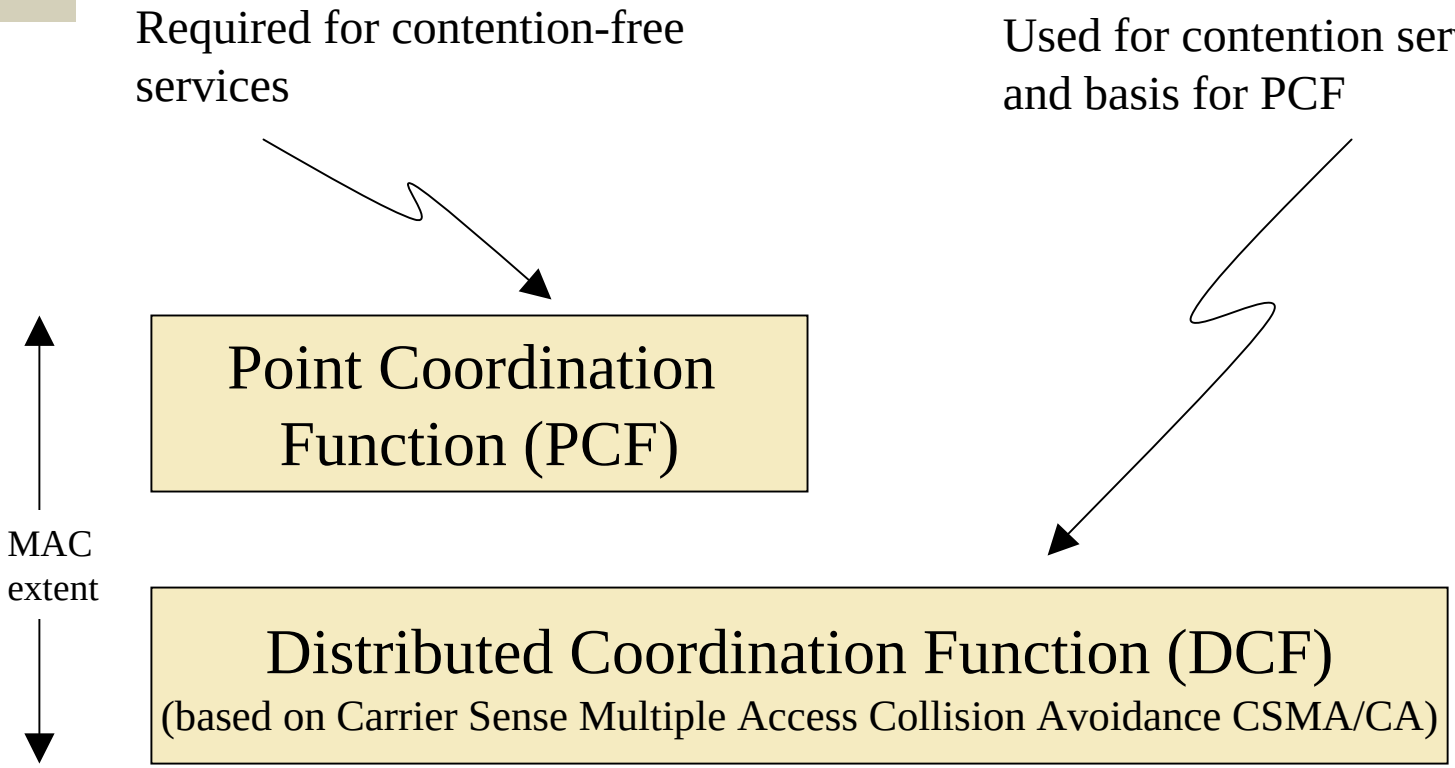
802.11 Medium Access Control (MAC) (1)



- address may be BSSID, Destination Address (DA), Source Address (SA), Receiver Address (RA) or Transmitter Address (TA)
- Each of addresses contain a 48-bit address
- MAC sublayer address is one of the following:
  - individual address
  - group address (multicast-group address or broadcast address)

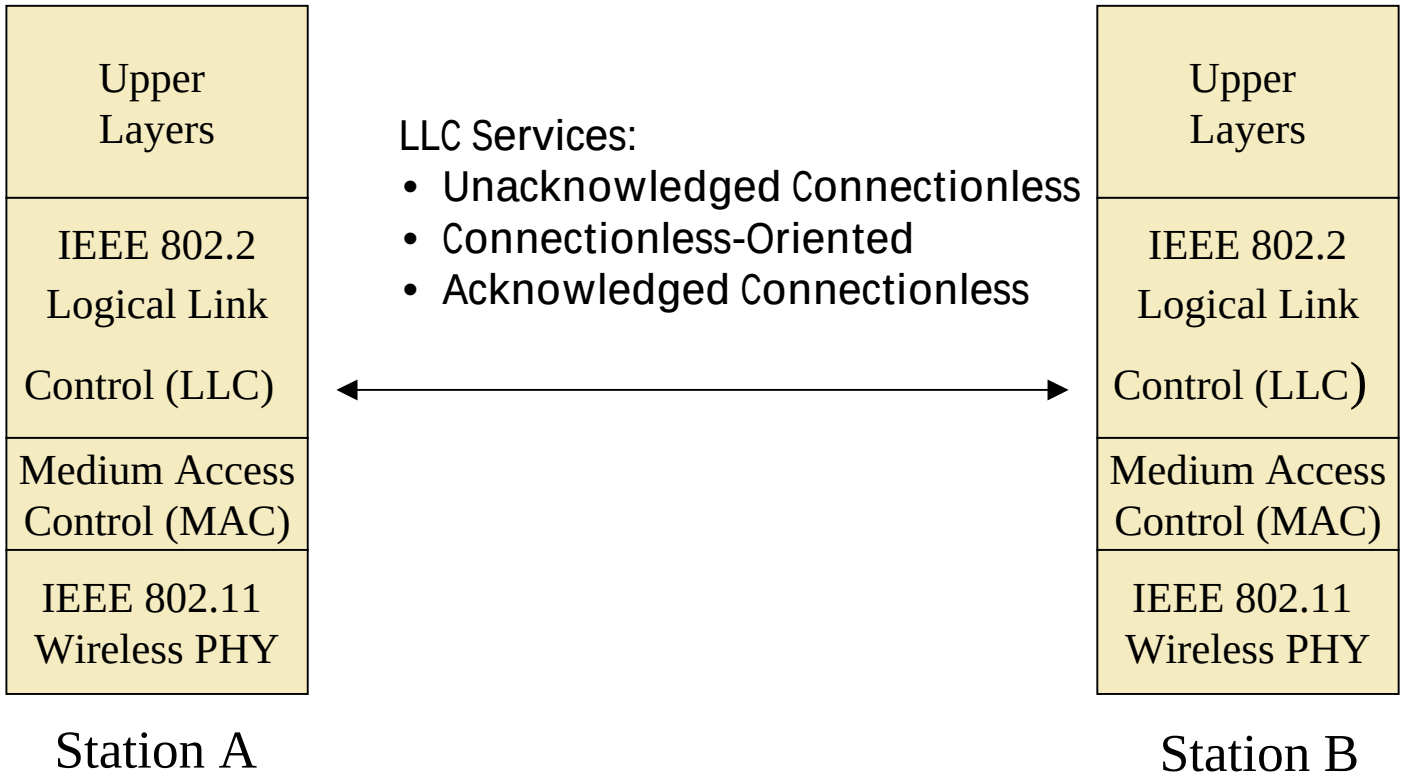
Standard IEEE 802.11 MAC Frame Format

802.11 Medium Access Control (MAC) (2)



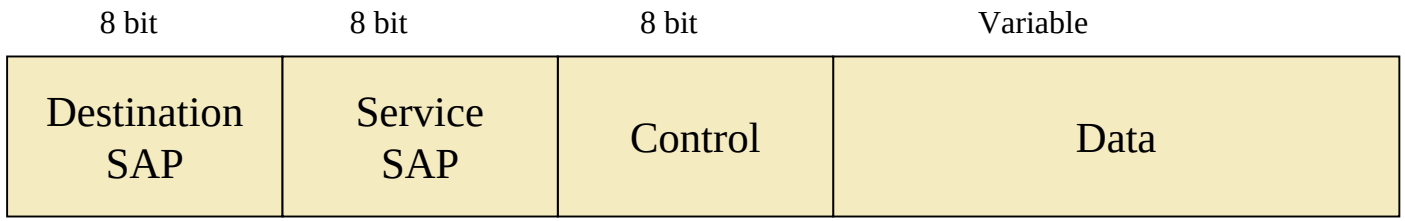
MAC Architecture

IEEE 802.11 LLC Services



The LLC provides end-to-end link control over an 802.11-based Wireless LAN.

IEEE 802.11 LLC PDU Structure



Control field indicates the type of the frame:

- *Information*: used to carry user data
- *Supervisory*: used for flow control and error control
- *Unnumbered*: various protocol control PDUs

IEEE 802.2 LLC Services

- Unacknowledged connectionless service
  - Higher layers must take care of error and flow control mechanisms
  - Peer-to-peer, multicast and broadcast communication
- Connection-oriented service
  - Error and flow control
  - Peer-to-peer communication
- Acknowledged connectionless service
  - Flow and error control with stop-and wait ARQ
  - Peer-to-peer, multicast and broadcast communication

IEEE 802.11a Physical Layer

- Describes WLANs for the 5-GHz band, with a data rate of 54Mbps
- Frequency Ranges
  - 5.15-5.25 GHz, 5.25-5.35 GHz, 5.725-5.825 GHz
- Modulation Method
  - OFDM System with 52 sub-carries using binary or quadrature phase-shift keying (BPSK/QPSK), 16-quadrature amplitude modulation (16-QAM) or 64-QAM
- Bit rates
  - 6, 9, 12, 18, 24, 36, 48 or 54 Mbps (6, 12 and 24 Mbps are mandatory)
- Forward error correction (convolutional coding) with ½, 2/3 or ¾ coding rates

IEEE 802.11b

- WLANs in the 2.4-GHz (2.4000-2.4835 GHz) band
- Data rate of 5.5 Mbps and/or 11 Mbps
- This was basically the first practical high speed data rate version of the 802.11 WLAN solutions

IEEE 802.11d Principals

- Based on 802.11 (1999) and 802.11a-1999 & 802.11b-1999 amendments
- Enables 802.11 hardware to work in various countries where it can't today.
- This amendment specifies the extensions to IEEE Std 802.11 or Wireless Local Area Networks providing specifications for conformant operation beyond the original six regulatory domains of that standard.
  - These extensions provide a mechanism for an IEEE Std 802.11 access point to deliver the required radio transmitter parameters to an IEEE Std 802.11 mobile station, which allows that station **to configure its radio to operate within the applicable regulations of a geographic or political subdivision**.
  - This mechanism is applicable to all IEEE Std 802.11 PHY types. A secondary benefit of the mechanism described in this amendment is the ability for an IEEE Std 802.11 mobile station **to roam between regulatory domains**.

IEEE 802.11d Change Details

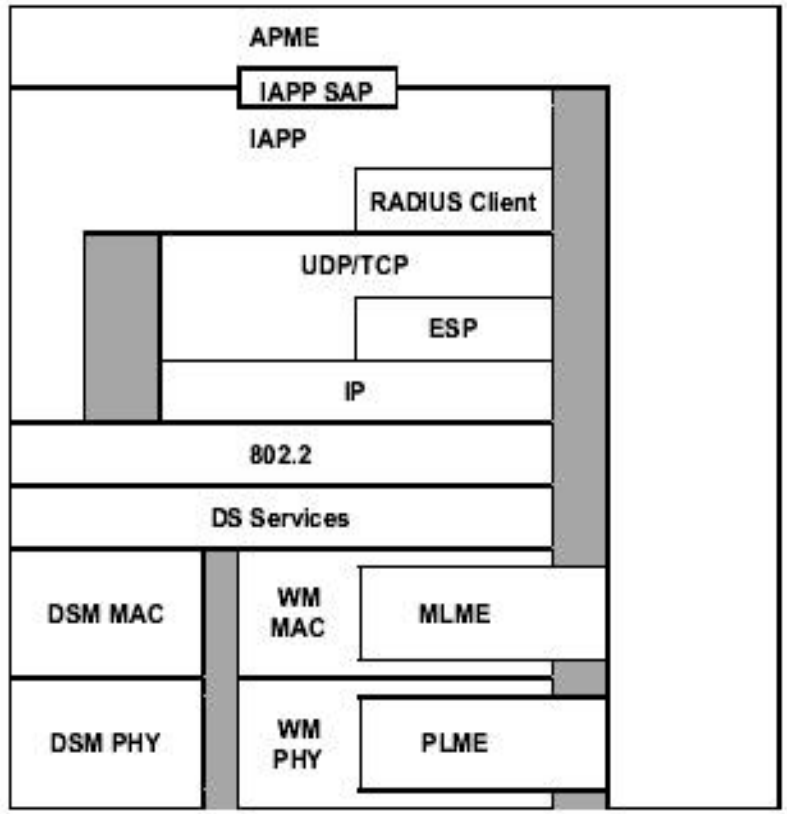
- Beacon Frame Body, Probe Message Body
  - Structures specified to contain: Country information and Frequency Hopping (FH) information
  - Contents of the Country Information Elements (CIE)
- MAC sub-layer specification:
  - Operation upon entering a regulatory domain
  - Suport for frequency hopping PHYs
  - Determining hopping patterns
- MAC sub-layer management
  - Initializing a BSS and synchronizing with a BSS
- Frequency Hopping Spread Spectrum (small editorial)
  - Frequency hopping pattern may be received as the frequency hopping table information from beacon or Probe Response frame

IEEE 802.11e

- Enhances the 802.11 Media Access Control layer for quality-of-service features, such as prioritizing voice or video traffic

IEEE 802.11f IAPP Protocol

- Recommends practices for WLAN equipment makers so that all their 802.11 access points can interoperate.
- IAPP protocol is planned for Distribution System (DS) in order IAPP to provide the necessary capabilities to achieve multi-vendor Access Point (AP) interoperability



IEEE 802.11f Specific

- Recommended practices for implementation of an Inter-Access Point Protocol (IAPP)on a Distribution System (DS) supporting ISO/IEC 8802-11:1999 and IEEE 802.11™ wireless local access network (WLAN) links are described.
- The recommended DS utilizes an IAPP that provides the necessary capabilities to achieve multi-vendor Access Point (AP) interoperability within the DS.
- This IAPP is described for a DS consisting of IEEE 802 LAN components utilizing an Internet Engineering Task Force (IETF) Internet Protocol (IP) environment.
- Throughout this recommended practice, the terms ISO/IEC 8802-11:1999, IEEE 802.11, 802.11™, and IEEE Std 802.11™-1999 are used interchangeably to refer to the same document, ISO/IEC 8802-11:1999, and its amendments and supplements published at the time this recommended practice was adopted.
- (Year 2003 release: experimental, open for commenting)

IEEE 802.11g

- Operates in the 2.4-GHz (2.4000-2.4835 GHz) band
- Uses 802.11a modulation to reach 54Mbps data rate
- Conceptually and physically combination of 802.11b and 802.11a, except that 802.11g operates (only) in the 2.4-GHz band

IEEE 802.11n Specific

- Designed to boost throughput, not raw data rate, to 100M bit/sec. The idea is to make WLANs feel like 100M bit/sec switched Ethernet LANs
- IEEE 802.11n will promote the idea that wired networks can be replaced with wireless technologies. One reason to embrace them is that high-throughput WLANs will eliminate cabling costs.
- The 802.11n task group's first order of business will be to define a group of application scenarios, describing how the high-throughput technology will be used.

IEEE 802.11i Features (1)

- One of the major tasks for 802.11i is to shore up the link-layer security of wireless networks. In the short term, security is improved by adding a enhancements on to standard RC4-based WEP.
- WPA ensures that TKIP keys vary for each packet through key mixing. WPA also increases part of the keyspace and adds encrypted packet integrity to reject inserted packets. Current Wi-Fi puts weak integrity outside the encrypted payload.
- Many in the industry views WPA as a stopgap measure intended mainly to buy time to get link-layer security right. 802.11i has always included a privacy algorithm based on the Advanced Encryption Standard (AES). It has always been a stated goal that the AES-based encryption in 802.11i should offer the strongest level of privacy possible. One way that the goal is often phrased is that 802.11i should offer security mechanisms that allow deployment of 802.11 networks without requiring extra network components for encryption. Put another way, 802.11i is designed to offer cryptographic security over the air equivalent to IPSec.

IEEE 802.11i Features (2)

- 802.11i includes both RC4-based encryption (the collection of protocol mechanisms that make up WPA) and the AES-based algorithm called the Counter Mode CBC-MAC Protocol (CCMP). The flawed design of WEP, and fact that WPA is simply a patch, make it unlikely that WPA would ever gain FIPS approval. CCMP is based on a FIPS-approved cipher, and is the future of wireless security at the link layer. However, CCMP cannot currently become FIPS-approved because it uses an unapproved mode.
- WPA includes full support for server-based authentication using the 802.1x protocol and EAP (Extensible Authentication Protocol), both part of the interim 802.11i draft.
- The Wi-Fi Alliance's decision to take a snapshot of the ongoing work of IEEE 802.11i committee's work on the ultimate standard carries inherent risk.
- Although there is no guarantee that products after February that adhere to the WPA standard will also be compatible with the final 11i security solution -- which isn't expected until the end of 2003 at the earliest

Homework

a. List and briefly define the IEEE 802.11 Protocol Layers
b. List and briefly define LLC services
c. Is a distribution system a wireless network?
d. What is portal in context with IEEE 802.11?
e. What are the frequency band, bit rates and modulation methods for:
    1) 802.11
    2) 802.11a
    3) 802.11b
    4) 802.11g