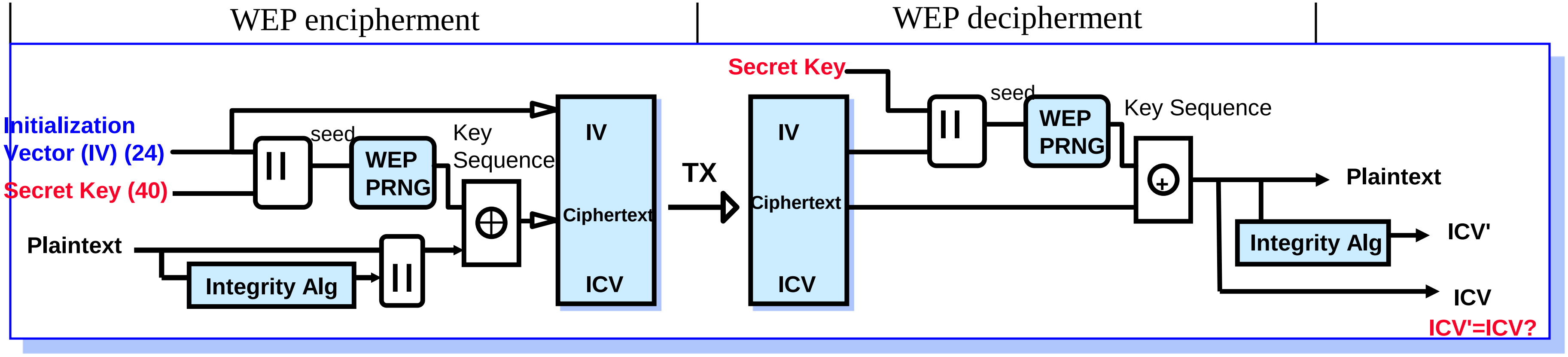
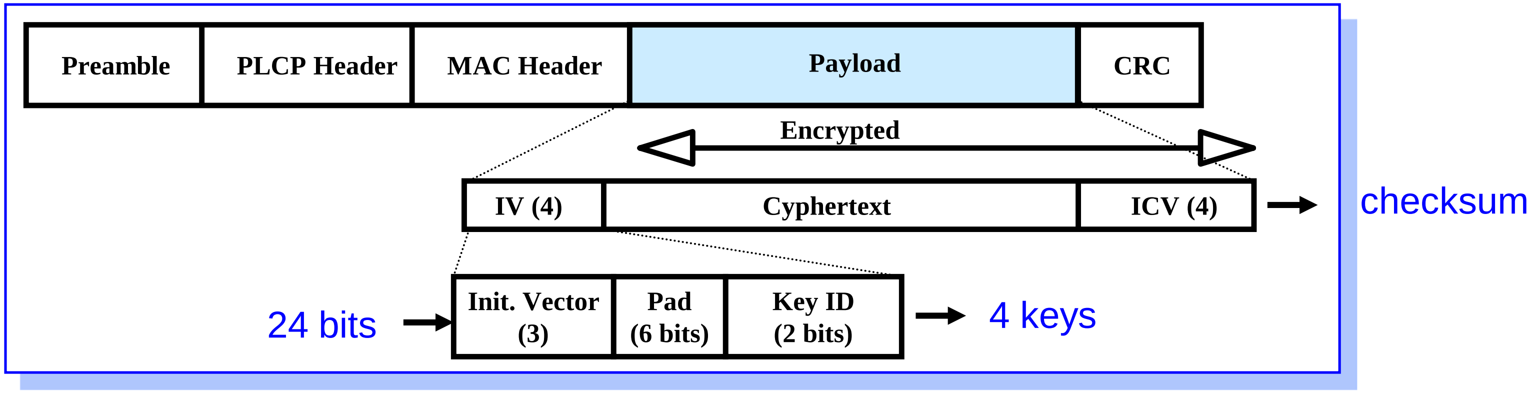
Privacy and Access Control

- Goal of 802.11 is to provide Wired Equivalent Privacy (WEP)
  - Usable worldwide
- 802.11 provides for an Authentication mechanism
  - To aid in access control.
  - Has provisions for OPEN Shared Key or proprietary authentication extensions.
- Optional (WEP) Privacy mechanism defined by 802.11.
  - Limited for Station-to-Station traffic, so not “end to end”.
    - » Embedded in the MAC entity.
  - Only implements Confidentiality function.
  - Uses RC4 PRNG algorithm based on:
    - » a 40-bit secret key (No Key distribution standardized)
      - by external key management service
    - » and a 24-bit IV that is send with the data.
    - » 40+24 = 64-bit PRNG seed (new 128, 152 bits - performane)
    - » includes an ICV to allow integrity check.
  - Only payload of Data frames are encrypted.
    - » Encryption on per MPDU basis.

Integrity Check Value (ICV) Initialization Vector (IV)

Privacy Mechanism





- WEP bit in Frame Control Field indicates WEP used.
  - Each frame can have a new IV, or IV can be reused for a limited time.
  - If integrity check fails then frame is ACKed but discarded.

Privacy Service (1/2)

- **Privacy**:
  - The service used to prevent the contents of messages from being reading by other than the intended recipient.
- In a wired LAN, only those stations physically connected to the wire can hear LAN traffic.
  - This is not true for the 802.11 wireless LAN.
- IEEE 802.11 provides the ability to encrypt the contents of messages.
- A MIB function is provided to inquire the encryption algorithms supported by a station.
- A mutually acceptable privacy algorithm must be agreed upon before an Association can be established.

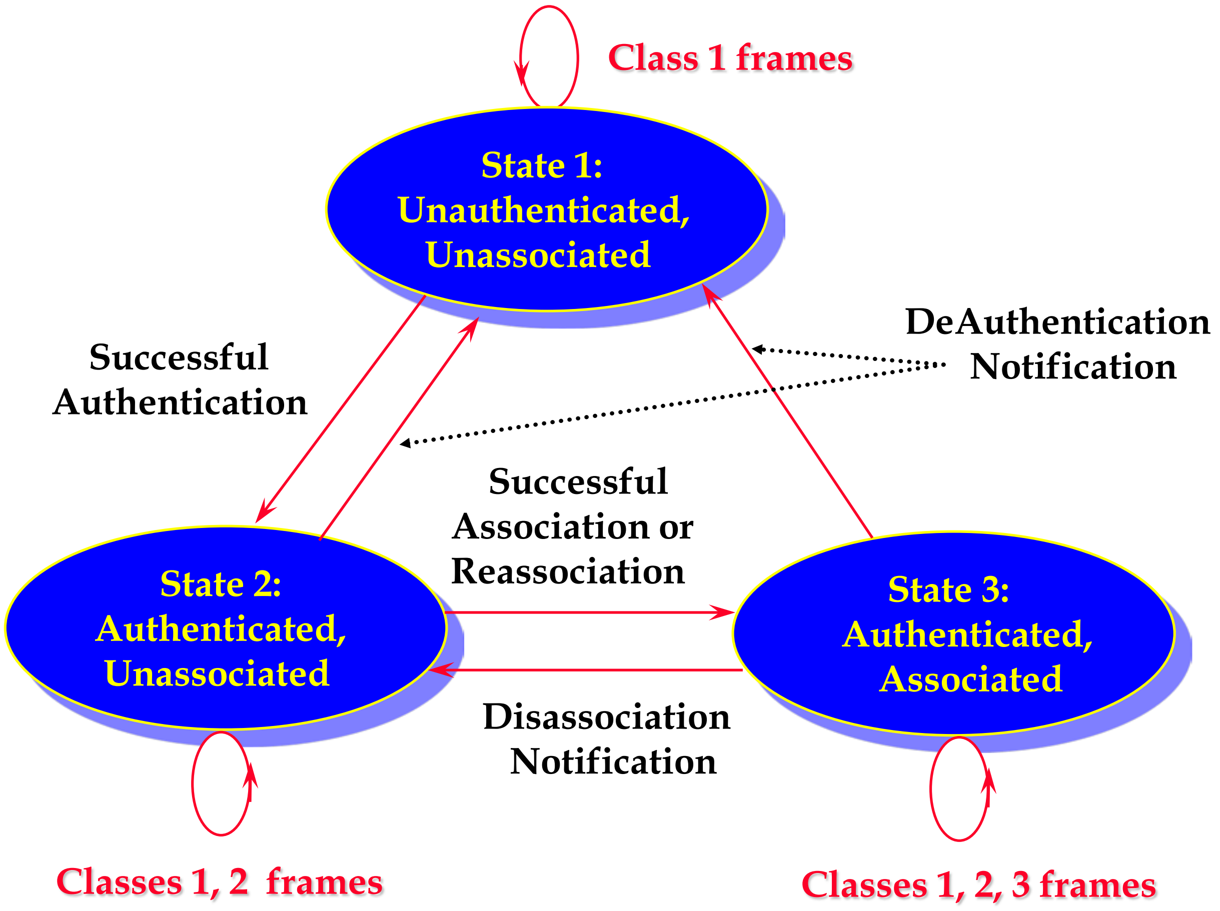
Privacy Service (2/2)

- The default privacy algorithm for all 802.11 stations is in the clear. If the privacy service is not invoked to set up a privacy algorithm, all messages will be sent unencrypted.
- If a privacy algorithm is set up, then the algorithm will be used for all subsequent transmissions.
- Even if an Association is successful, a later Reassociation may be refused.
- 802.11 specifies an optional privacy algorithm that is designed to satisfy the goal of wired LAN "*equivalent* " privacy.

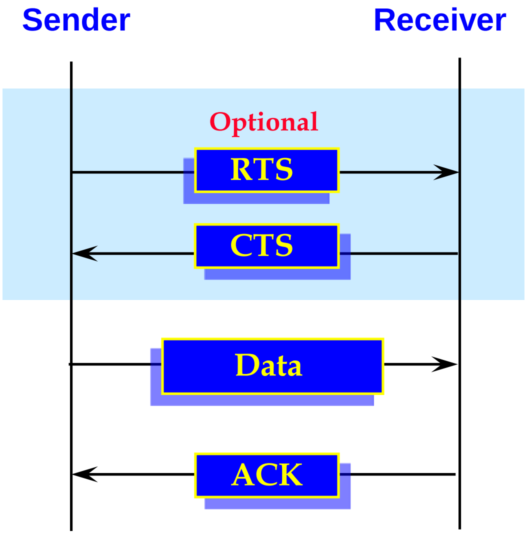
Relationship Between Services

- For a station, two state variables are required to keep track:
  - Authentication State : Unauthenticated and Authenticated
  - Association State : Unassociated and Associated
- Three station states are possible:
  - State 1 : Initial start state, Unauthenticated, Unassociated.
  - State 2 : Authenticated, not Associated.
  - State 3 : Authenticated and Associated
- These states determine the 802.11 frame types (grouped into classes) which may be sent by a station.
  - State 1 : Only Class 1 frames are allowed.
  - State 2 : Either Class1 or Class 2 are allowed.
  - State 3 : All frames (Class 3) are allowed.

Relationship Between State Variables and Services



Frame Types



- Class 1 frames
  - Control Frames
    - (1) RTS
    - (2) CTS
    - (3) ACK
    - (4) CF-End+ACK
    - (5) CF-End
  - Management Frames
    - (1) Probe Request/Response
    - (2) Beacon
    - (3) Authentication
      - Successful association enables Class 2 frames.
      - Unsuccessful association leaves STA in State 1.
    - (4) Deauthentication

      Return State 1.
    - (5) Announcement traffic indication message (ATIM)
  - Data Frames
    - (1) In IBSS, direct data frames only (FC control bits "To DS and from DS" both false)

Frame Types

- Class 2 Frames
  - Data Frames

    (1) Asynchronous data. Direct data frames only (FC control bits "To DS and from DS" both false)
  - Management Frames

    (1) Association Request/Response
    - » Successful association enables Class 3 frames.
    - » Unsuccessful association leaves STA in State 2.

    (2) Reassociation request/response
    - » Successful association enables Class 3 frames.
    - » Unsuccessful association leaves STA in State 2.

    (3) Disassociation

    Return State 2.

PS. When STA A receives a non-authenticated frame from STA B, STA A sends a deauthentication to STA B

Frame Types

- Class 3 Frames
  - Data Frames

    (1) Asynchronous data. Indirect data frames allowed (FC control bits "To DS and from DS" may be set to utilize DS Services)

  - Management Frames

    (1) Deauthentication

      - » Return state 1

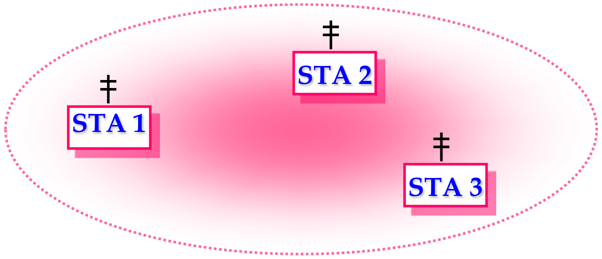
  - Control Frames

    (1) PS-Poll

Differences Between ESS and Independent BSS LANs

- An independent BSS (IBSS) is often used to support an "Ad-Hoc" network, in which a STA communicates directly with one or more other STAs.
- IBSS is a logical subset of an ESS and consists of STAs which are directly connected.
- Since there is no physical DS, there cannot be a Portal, an integrated wired LAN, or the DS Services.
- In an IBSS, only class 1 frames are allowed since there is no DS in an IBSS.
- The services which apply to an IBSS are the Station Services.

1. Authentication
2. Deauthentication
3. Privacy
4. MSDU delivery



IBSS

Frame and MPDU Formats

- Each frame should consist of three basic components:
  - A MAC Header, which includes control information, addressing, sequencing fragmentation identification, duration, and QoS information.
  - A variable length Frame Body, which contains information specify to the frame type.
  - A frame check sequence (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).

Frame Formats

Octets: 2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame Body	CRC

802.11 MAC Header

Bits: 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	SubType	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order / rsrv

Frame Control Field

- MAC Header format differs per Type:
  - Control Frames (several fields are omitted) 1 or 2 address field
  - Management Frames 3 address fields
  - Data Frames 4 address fields
- Includes Sequence Control Field for filtering of duplicate caused by ACK mechanism.

Address Field Description

To DS	From DS	Address 1	Address 2	Address 3	Address 4	
0	0	DA	SA	BSSID	N/A	→ Ad hoc
0	1	DA	BSSID	SA	N/A	→ From AP
1	0	BSSID	SA	DA	N/A	→ To DS
1	1	RA	TA	DA	SA	→ Wireless Bridge

- Addr 1 = All stations filter on this address.
- Addr 2 = Transmitter Address (TA)
  - Identifies transmitter to address the ACK frame to.
- Addr 3 = Dependent on *To* and *From DS* bits.
- Addr 4 = Only needed to identify the original source of WDS (*Wireless Distribution System)* frames.
  - BSSID
    - infrastructure : AP MAC address
    - Ad Hoc : 01 + 46-bit random number (may set as '1')

Frame Fields

- Frame Control Field :
  - Protocol Version: the value of the protocol version is zero.

    A device that receives a frame with a higher revision level than it supports will discard the frame without indication to the sending STA or to LLC.
  - Type and Subtype: used to identify the function of the frame.
  - To DS: is set to 1 in data type frames destined for the DS via AP.
  - From DS: is set to 1 in data type frames existing the DS.
  - More Fragment: is set to 1 if there has another fragment of the current MSDU or MMSDU.
  - Retry : Indicates that the frame is a retransmission of an earlier frame. A station may use this indication to eliminate duplicate frames.
  - Power Management : Indicates power management mode of a STA.
    - A value of 1 indicates that the STA will be in power-save mode.
    - A value of 0 indicates that the STA will be in active mode.
    - This field is always set to 0 in frames transmitted by an AP.

Frame Fields

- More Data: is used to indicate to a STA in power-save mode that more MSDUs, or MMSDUs are buffered for that STA at the AP; or indicate that at least one additional MSDU buffered at STA available for transmission in response to a subsequent CF-Poll
- WEP: It is set to 1 if the Frame Body field contains information that has been processed by the WEP algorithm.
- Order: is set to 1 in any data type frame that contains an MSDU, or fragment, which is being transferred using the Strictly Ordered service class.

- Duration or Connection ID : Used to distribute a value (us) that shall update the Network Allocation Vector (NAV) in stations receiving the frame.

Duration/ID Field

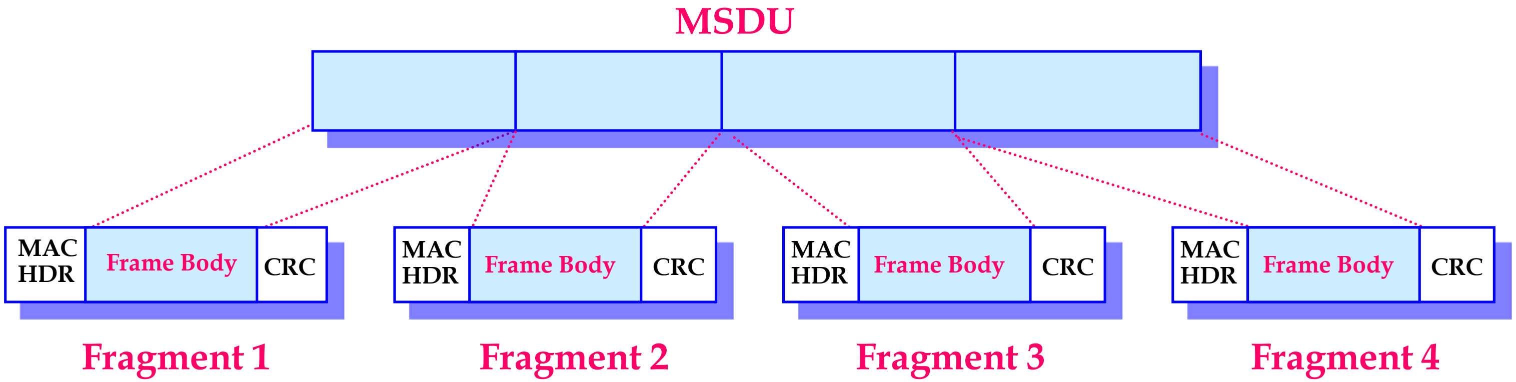
- In PS-Poll control frame, Duration/ID carries association ID (AID) with the 2 MSB set as 1 (AID range 1-2007)
- Other types carries duration in us.
- Transmitted frames in CFP, duration is set as 32768.

Bit 15	Bit 14	Bits 13-0	Usage
0	0-32767		Duration (us)
1	0	0	Fixed value within frames transmitted during the CFP
1	0	1-16383	Reserved
1	1	0	Reserved
1	1	1-2007	AID in PS-Poll frames
1	1	2008-16383	Reserved

→ 2007 STAs

Frame Fields

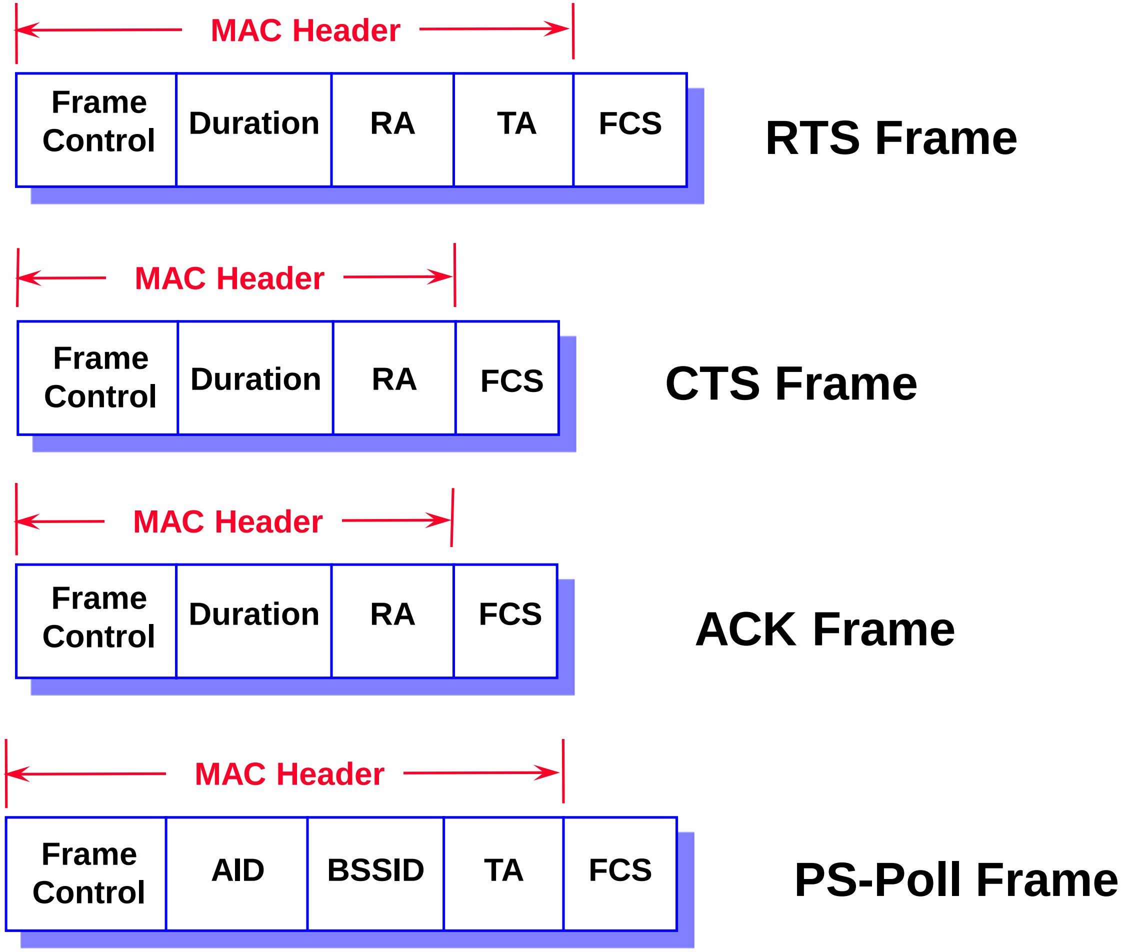
- Address Fields : Indicate the BSSID, SA, DA, TA (Transmitter address), RA (Receiver address), each of 48-bit address.
- Sequence Control
  - – Sequence Number (12-bit): An incrementing value. The same value shall be used for all fragments of the same MSDU.
  - – Fragment Number (4-bit): Indicates the number of each individual fragment. → At least 16 fragments → More Fragment field
- Frame Body: 0 – 2312 bytes.
- CRC (4 octets)



Format of Individual Frame Types

- Control Frames
  - *Immediately previous* frame means a frame, the reception of which concluded within the prior SIFS interval.
- RTS Frame Format
  - In an infrastructure LAN, the DA shall be the address of the AP with which the station is associated.
  - In an ad hoc LAN, the DA shall be the destination of the subsequent data or management frame.
- CTS Frame Format
  - The DA shall be taken from the source address field of the RTS frame to which the CTS is a response.
- ACK Frame Format
  - The DA shall be the address contained in the Address 2 field of the immediately previous Data or Management frame.
- PS-Poll Frame Format
  - The BSS ID shall be the address of the AP.
  - The AID shall be the value assigned by the AP in the Association Response frame.
  - The AID value always has its two significant bits set to 1. (Bit 14 and 15)

Format of Individual Frame Types (control frames)



Bit : 7654
Subtype: 1011

MAC Header

Frame Control	Duration	RA	TA	FCS

RTS Frame

Subtype: 1100

MAC Header

Frame Control	Duration	RA	FCS

CTS Frame

Subtype: 1101

MAC Header

Frame Control	Duration	RA	FCS

ACK Frame

Subtype: 1010

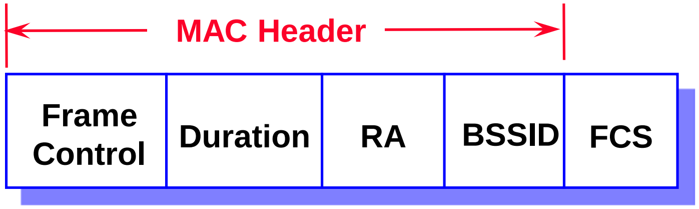
MAC Header

Frame Control	AID	BSSID	TA	FCS

PS-Poll Frame

Format of Individual Frame Types (control frames)

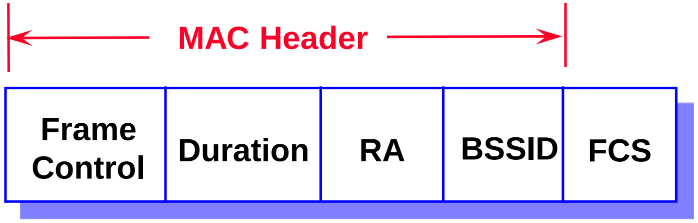
Bit: 7654
Subtype:1110



Frame Control	Duration	RA	BSSID	FCS

CF-End Frame

Subtype:1111



Frame Control	Duration	RA	BSSID	FCS

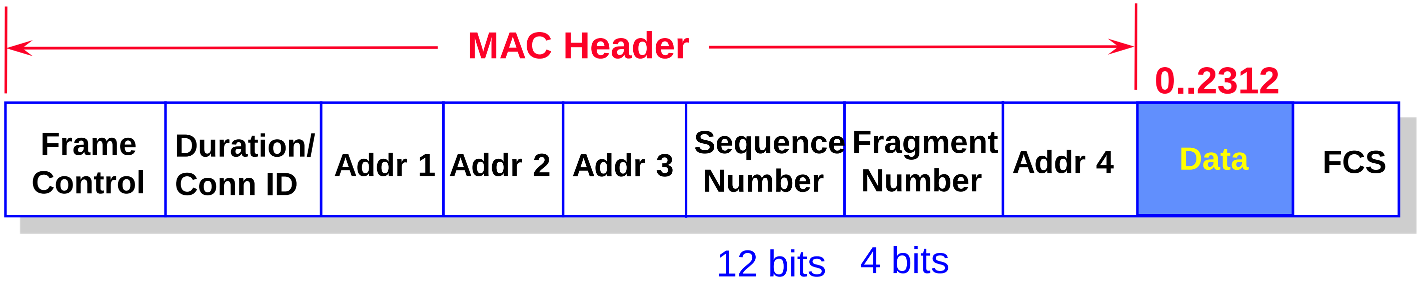
CF-End+CF-Ack Frame

- **The BSSID is the address of the STA contained in the AP.**
- **The RA is the broadcast group address.**
- **The Duration field is set to 0.**

Format of Individual Frame Types

- Data Frames
  - The contents of the Address fields shall be dependent upon the values of the To DS and From DS bits.
  - A station shall use the contents of Address 1 to perform address matching for receive decisions.
  - The DA shall be the destination of the frame (MSDU).
  - The RA shall be the address of the AP in the wireless DS that is the next immediate intended recipient of the frame.
  - The TA shall be the address of the AP in the wireless DS that is transmitting the frame.
  - The BSSID
    - » The AP address, if the station is an AP or associated with an AP.
    - » The BSS ID of the ad hoc LAN, if the station is a member of an ad hoc LAN.
  - The frame body is null (0 octets in length) in data frames of subtype null function (no data), CF-Ack (no data), CF-Poll (no data), and CF-Ack+CF-Poll (no data).

Data Frames



MAC Header

0..2312

Frame Control	Duration/ Conn ID	Addr 1	Addr 2	Addr 3	Sequence Number	Fragment Number	Addr 4	Data	FCS

12 bits 4 bits

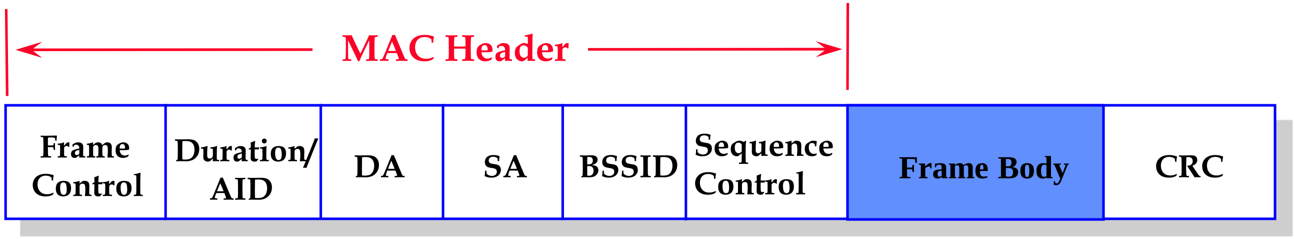
To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Frame Exchange Sequences

- The following frame sequences are possible:
  - Data
  - Data - ACK
  - RTS - CTS - Data - ACK
  - Data - ACK - Data - ACK (Fragmented MSDU)
  - RTS - CTS - Data - ACK - Data - ACK (Fragmented MSDU)
  - Poll - Data - ACK STA to AP
  - Poll - Data - ACK - Data - ACK (Fragmented MSDU)
  - Poll - ACK (No data) No data or More data
  - ATIM – ACK Ad hoc power saving
  - Request (management : Probe Request)
  - Request - ACK (management)
  - Response - ACK (management)
  - CTS - Data (11g)
  - CTS - Management (11g)
  - CTS - Data - ACK (11g)
  - CTS - Data - ACK - Data - ACK (Fragmented MSDU) (11g)

Format of Individual Frame Types

- **Management Frames**
  - The BSSID
    - » The AP address, if the station is an AP or associated with an AP.
    - » The BSS ID of the ad hoc LAN, if the station is a member of an ad hoc LAN.
  - The Frame body shall be the ***information elements***:



MAC Header

Frame Control	Duration/ AID	DA	SA	BSSID	Sequence Control	Frame Body	CRC

Management Frames (Frame Body)

- BEACON Frame: Time stamp, beacon interval, Capability information, SSID, supported rates, FH Parameter Set, DS parameter Set, CF Parameter Set, IBSS Parameter Set, and TIM. (the parameter sets are present only when the functions are used)
  - » In 802.11g, new "ERP Information Element" and "Extended Supported Rates Element"are added.
- ATIM Frame: Null
- Disassociation Frame: Reason code.
- Association Request Frame: Capability information, Listen Interval, SSID, and Supported Rates.
- Association Response Frame: Capability information, Status code, Association ID (AID), and the supported rates.
- Reassociation Request Frame: Capability information, Listen Interval, Current AP address, SSID, and Supported Rates.
- Reassociation Response Frame: Capability information. status code, Association ID (AID), and supported rates.
- Deauthentication: Reason code.

Management Frames (Frame Body)

- Probe Request Frame: SSID and the supported rates.
- Probe Response Frame: Time stamp, beacon interval, capability information, supported rates, and parameter sets.
  - » Omit "TIM" field.
  - » In 802.11g, new "ERP Information Element" and "Extended Supported Rates Element"are added.
- Authentication Frame: Authentication algorithm number (0:Open system 1: Shared Key), Authentication transaction sequence number, Status code (if reserved, set to 0), and Challenge text.

Authentication algorithm	Authentication Transaction sequence number	Status code	Challenge text
Open System	1	Reserved	Not present
Open System	2	Status	Not present
Shared Key	1	Reserved	Not present
Shared Key	2	Status	Present
Shared Key	3	Reserved	Present
Shared Key	4	Status	Not present

Capability Information field 1

2 octets

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10		B13		B15
ESS	IBSS	CF Pollable	CF-Poll Request	Privacy	Short Preamble	PBCC	Channel Agility			Short Slot time	…	DSSS-OFDM		
						802.11b				802.11g		802.11g		

- **APs** set the ESS subfiled to 1 and IBSS subfield to 0 within transmitted Beacon or Probe Response management frame.

- **STAs** within an IBSS set the ESS subfield to 0 and IBSS subfield to 1 in transmitted Beacon or Probe Response management frame.

- **Bit 10** is used to indicate 9us slot time is used. (IEEE 802.11g)

- **Bit 13** is used to indicate the new option of DSSS-OFDM. (IEEE 802.11g)

Capability Information field 2

2 octets

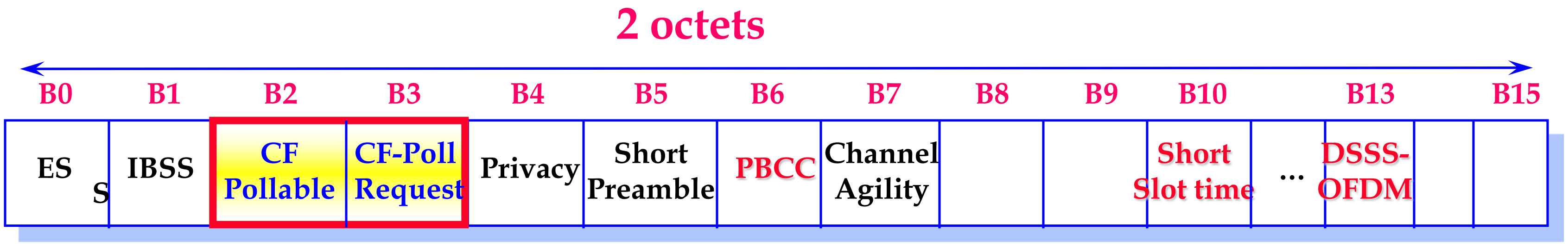
B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10		B13		B15
ES S	IBSS	CF Pollable	CF-Poll Request	Privacy	Short Preamble	PBCC	Channel Agility			Short Slot time	…	DSSS-OFDM		

801.11g

- **STAs set the CF-Pollable and CF-Poll Request subfields in Association Request and Reassociation Request management frames according to**

CF-Pollable	CF-Poll request	Meaning
0	0	STA is not CF-Pollable
0	1	STA is CF-Pollable, not requesting to be placed on the CF-Polling list
1	0	STA is CF-Pollable, requesting to be placed on the CF-Polling list
1	1	STA is CF-Pollable, requesting never to be Polled

Capability Information field 3



801.11g

- APs set the CF-Pollable and CF-Poll Request subfields in Beacon, Probe Response and Association Response, Reassociation Response management frames according to

CF-Pollable	CF-Poll request	Meaning
0	0	No point coordinator at AP
0	1	Point coordinator at AP for delivery only
1	0	Point coordinator at AP for delivery and polling
1	1	Reserved

Polling downlink

Polling downlink and uplink

Capability Information field 4

2 octets

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10		B13		B15
ES S	IBSS	CF Pollable	CF-Poll Request	Privacy	Short Preamble	PBCC	Channel Agility			Short Slot time	…	DSSS-OFDM		

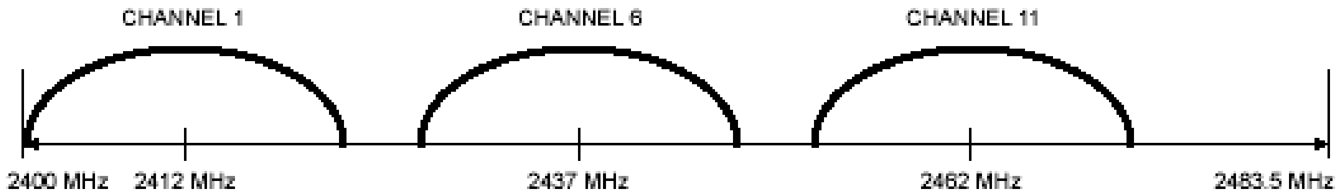
801.11g

- Optional frequency hopping for solve the shortcoming of static channel assignment in DSSS.
  - Example : Tone jammer
- Goal : without added cost
- Interoperability with 802.11 FHSS 1/2Mbps
  - Use same frequency hopping patterns

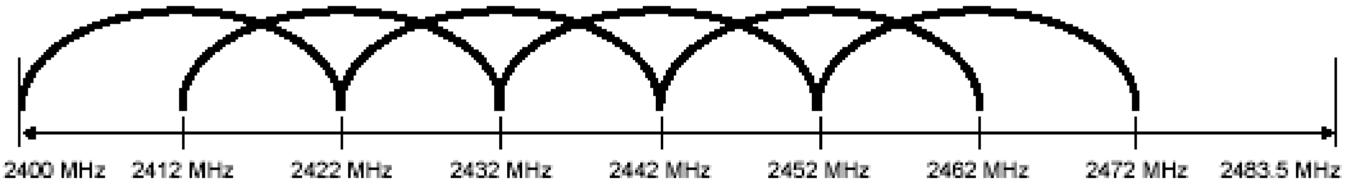
Channel Agility (optional)

- Two Sets for frequency hopping patterns (**224us per hop**)
  - North American

Set	Number of Channels	HR/DSSS Channel Number
1	3	1,6,11
2	6	1,3,5,7,9,11



Non-overlapping Channels Selection (25MHz gap)

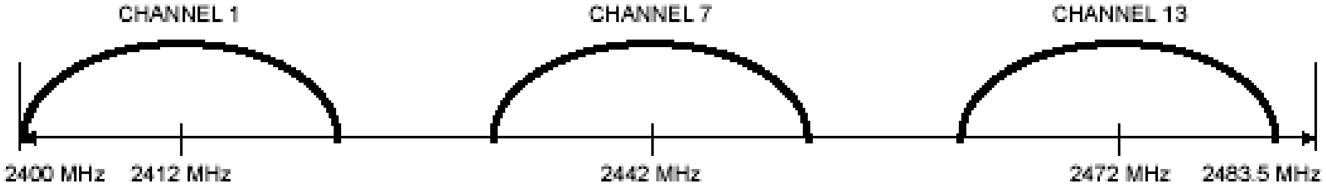


Half-overlapping Channels Selection (10MHz gap)

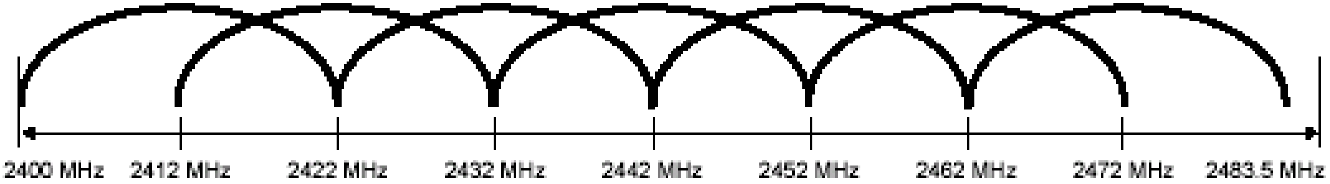
Channel Agility (optional)

- Two Sets for frequency hopping patterns
  - Europe (except Spain and France)

Set	Number of Channels	HR/DSSS Channel Number
1	3	1,7,13
2	7	1,3,5,7,9,11,13



Non-overlapping Channels Selection (30MHz gap)



Half-overlapping Channels Selection (10MHz gap)