Wireless LANs
June – September 2009

IEEE 802.11 MAC

รศ. ดร. อนันต์ ผลเพิ่ม

Assoc. Prof. Anan Phonphoem, Ph.D.

anan.p@ku.ac.th

Intelligent Wireless Network Group (IWING Lab)

http://iwing.cpe.ku.ac.th

Computer Engineering Department

Kasetsart University, Bangkok, Thailand

MAC Layer

- **MAC Layer operation**
  - Contention & contention-free
  - Priority frame transmission
- MAC frame structure
  - Create MAC frame
- MAC frame Types
  - MAC management, control, and data frame

MAC Layer Operations

- Accessing the wireless medium
  - IFS
  - PCF & DCF
- Joining the network
- Providing authentication and privacy

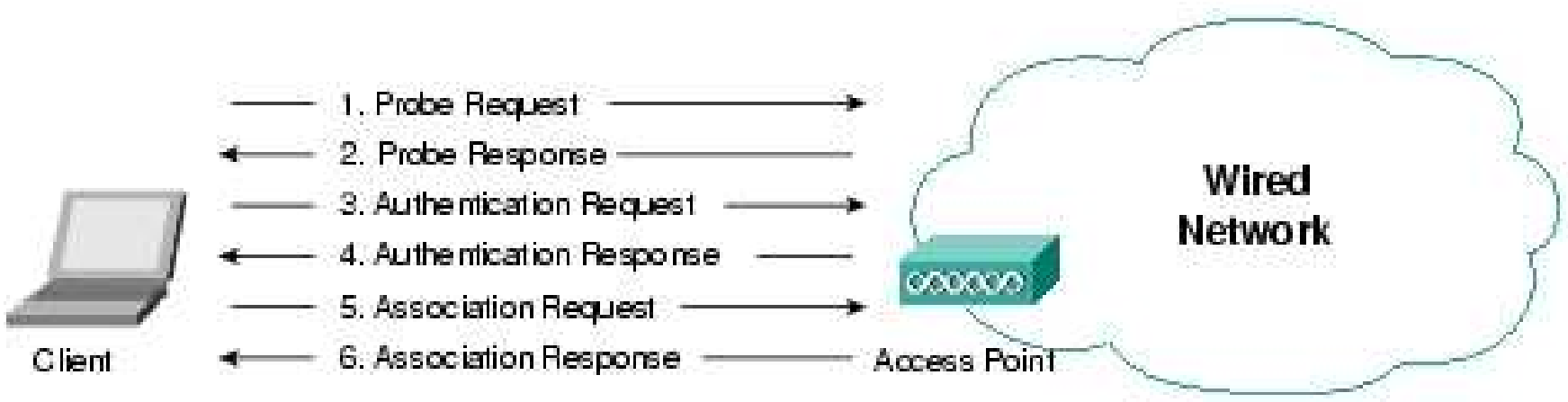
Startup/Joint the network

- Turn on → discovery phase
  - determine AP or other stations exist
- If exist → joint the network, get the following:
  - Service Set Id (SSID)
  - Timing Synchronization Function (TSF)
  - Timer Value
  - PHY setup parameters
- Negotiate for connection
  - Authentication & Association

Discovery Phase

- Enter scanning mode
  - Passive / Active scanning mode
- Passive
  - Listen for a Beacon for ChannelTime period
  - In Beacon → get the SSID & parameters
- Active
  - Transmit a **probe frame** (including the SSID that wishes to join)
  - Wait for a period responded by AP or other stations

802.11 Station Authentication



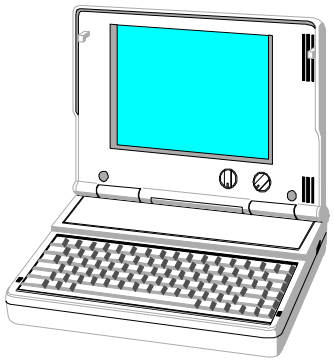
MAC Layer Operations

- Accessing the wireless medium
- Joining the network
- **Providing authentication and privacy**

Authentication

- Open system authentication
  - Default mode
- Shared key authentication
  - Higher degree of security
  - More rigorous frame exchange
  - Need to implement WEP

Open System Authentication



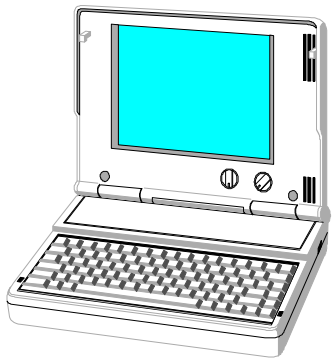
Initiating Station

Request

Authentication Frame
Algorithm = “Open”
Seq. No. = 1

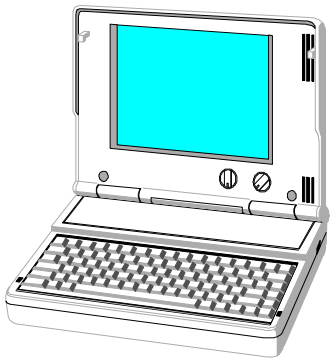
Accept/Reject

Authentication Frame
Algorithm = “Open”
Seq. No. = 2
Result = accept/Rej



Authenticating Station

Shared Key Authentication



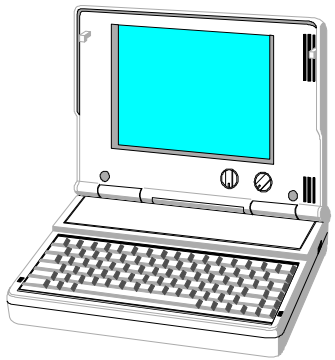
Initiating Station

Algorithm = “Shared Key”
Seq. No. = 1

Algorithm = “Shared Key”
Seq. No. = 2
Challenge Text

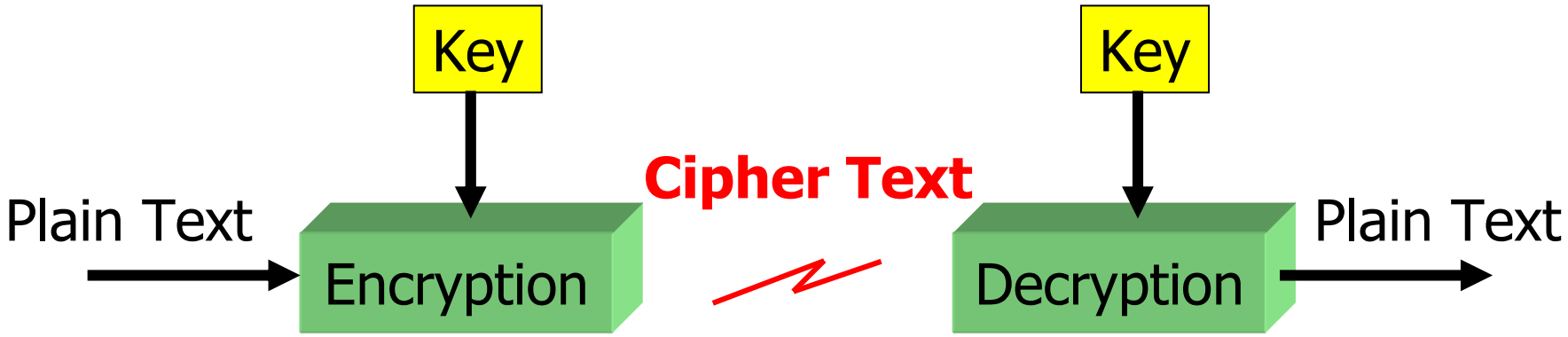
Algorithm = “Shared Key”
Seq. No. = 3
Encrypt Challenge Text

Algorithm = “Shared Key”
Seq. No. = 4
Authen result



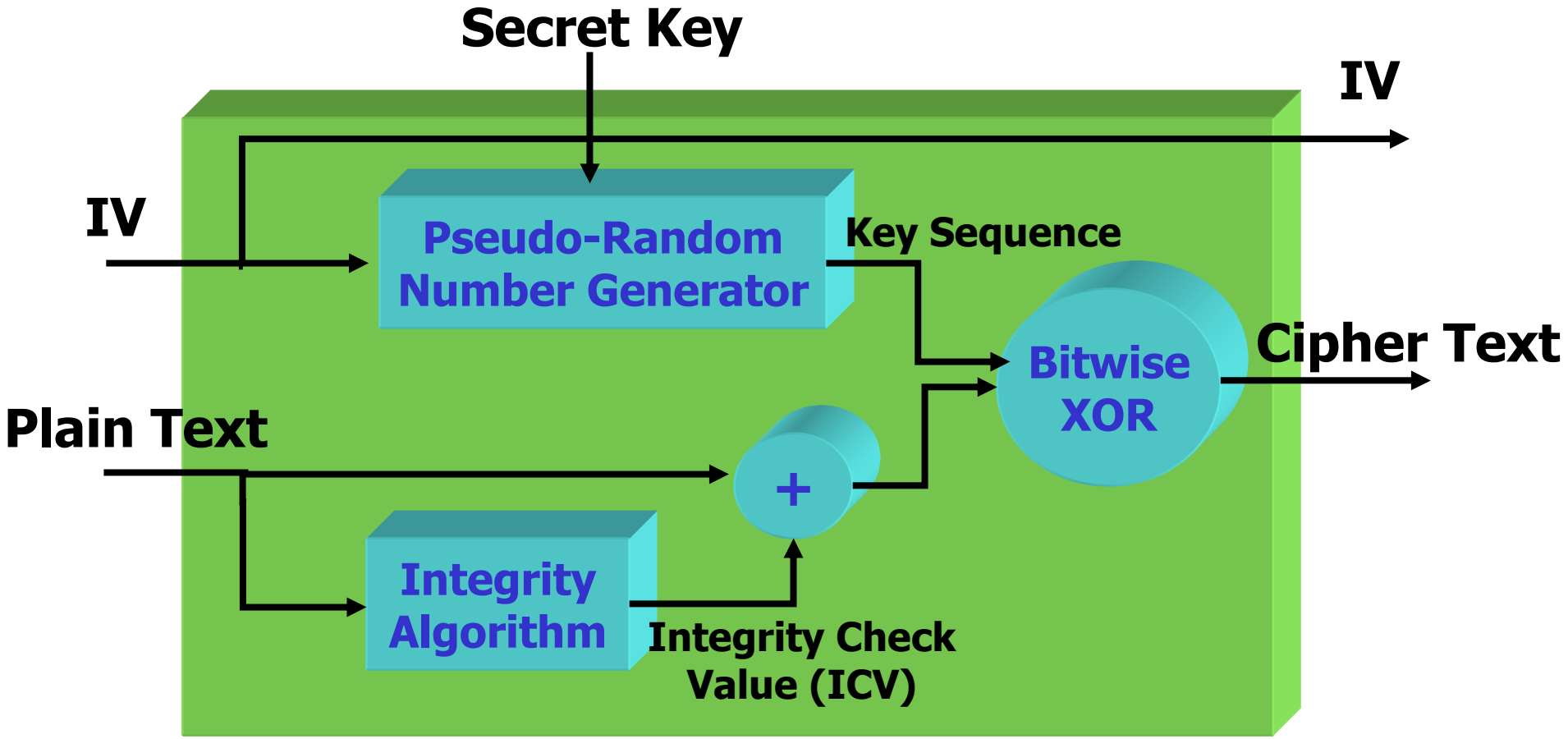
Authenticating Station

Wired Equivalent Privacy

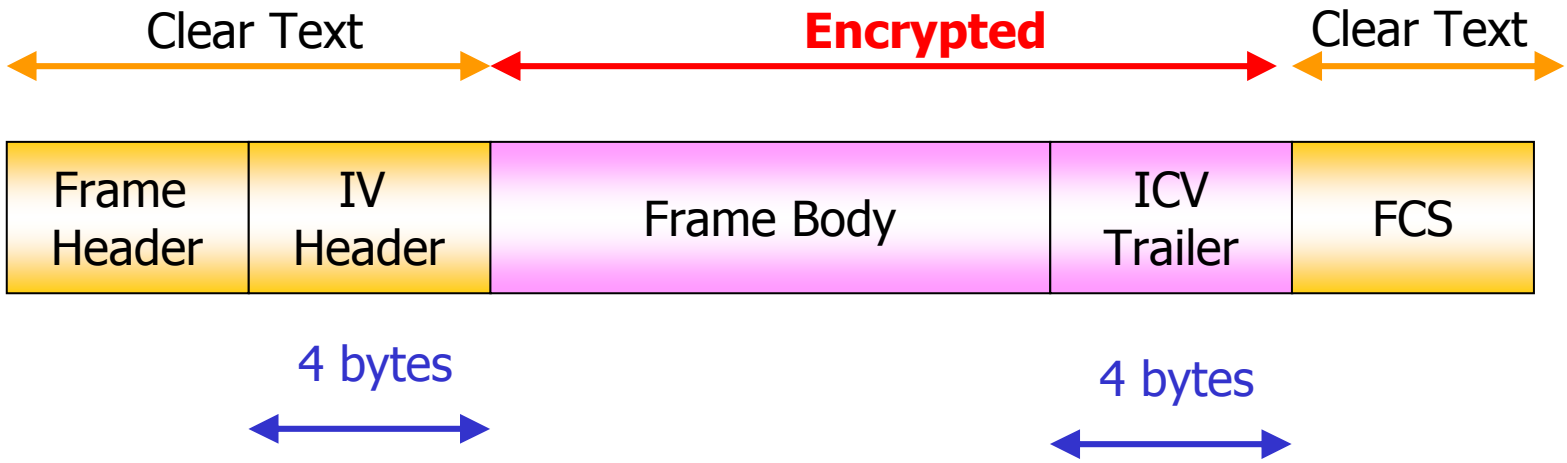


Symmetric Encryption

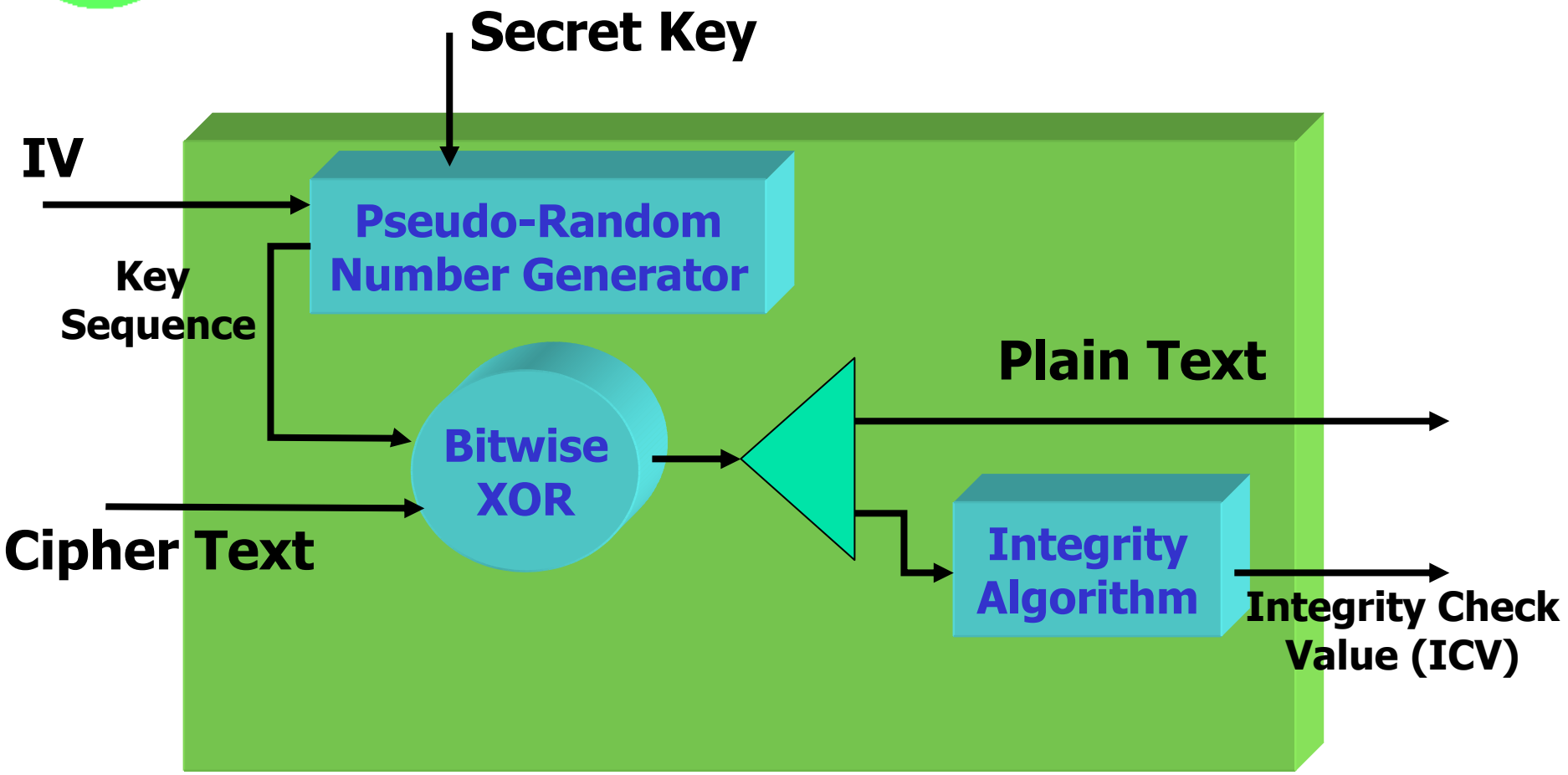
WEP - Encryption



WEP Frame


Clear Text
Encrypted
Clear Text
Frame Header
IV Header
Frame Body
ICV Trailer
FCS
4 bytes
4 bytes

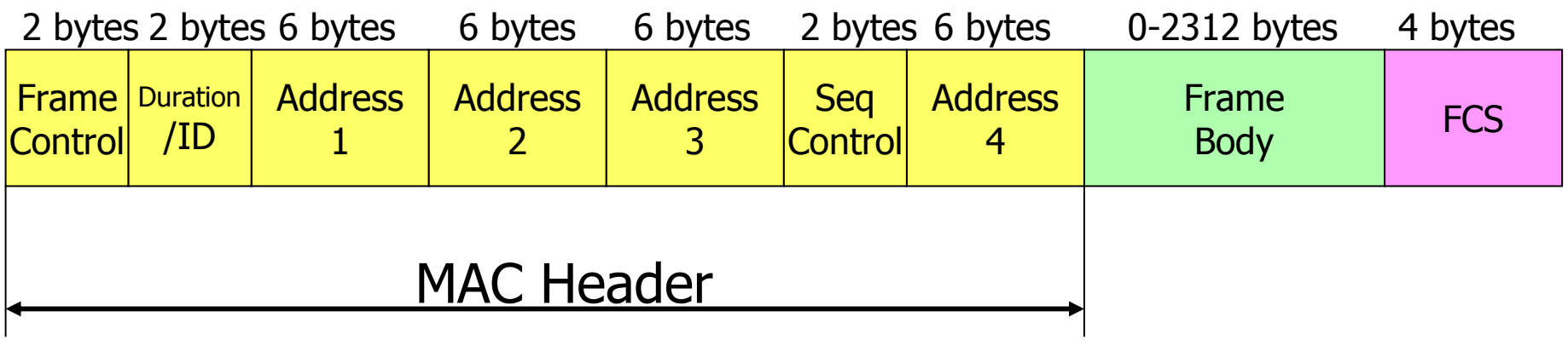
WEP - Decryption



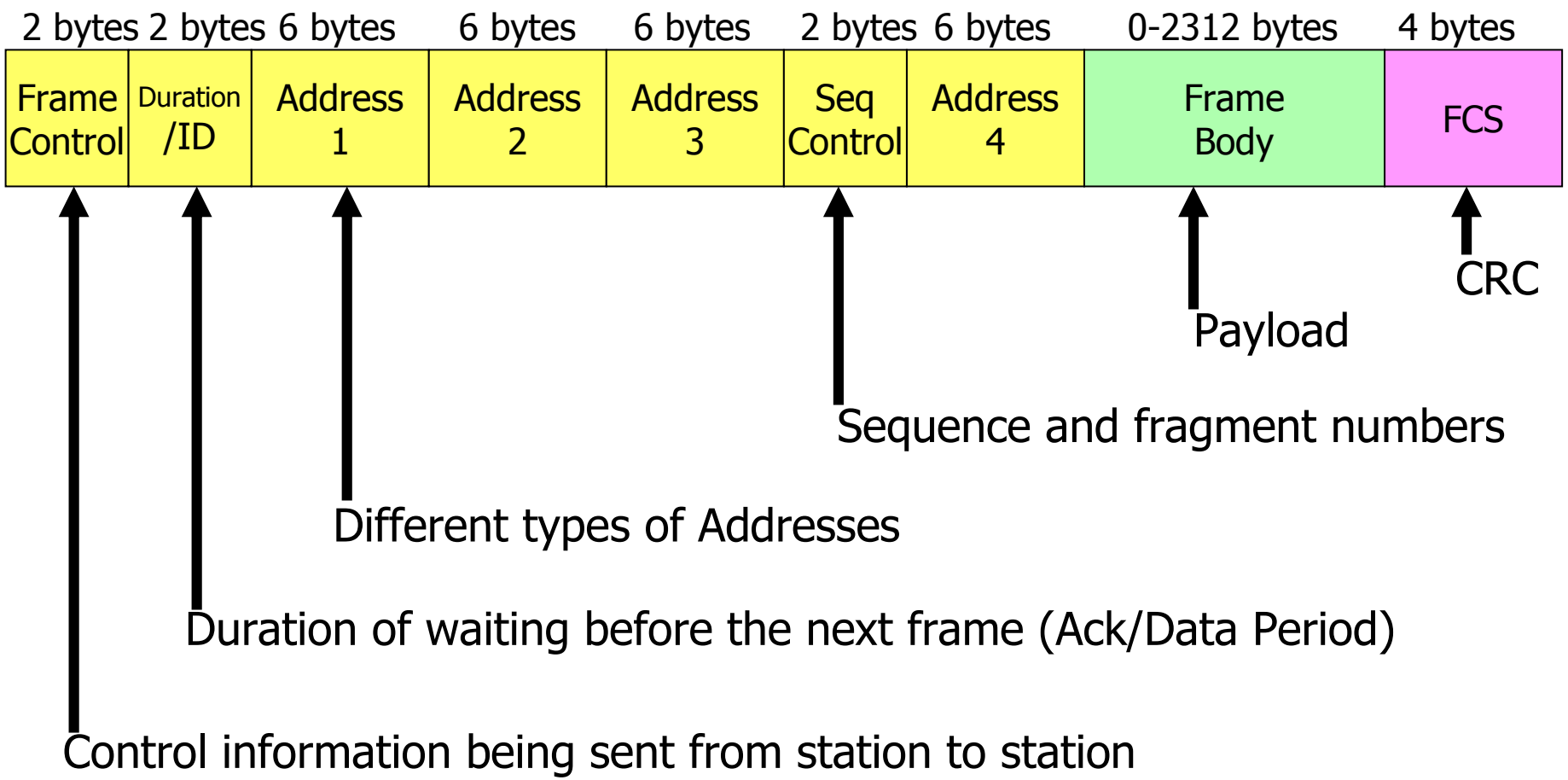
MAC Layer

- MAC Layer operation
  - Contention & contention-free
  - Priority frame transmission
- **MAC frame structure/Types**
  - MAC management, control, and data frame
- Basic process revisit

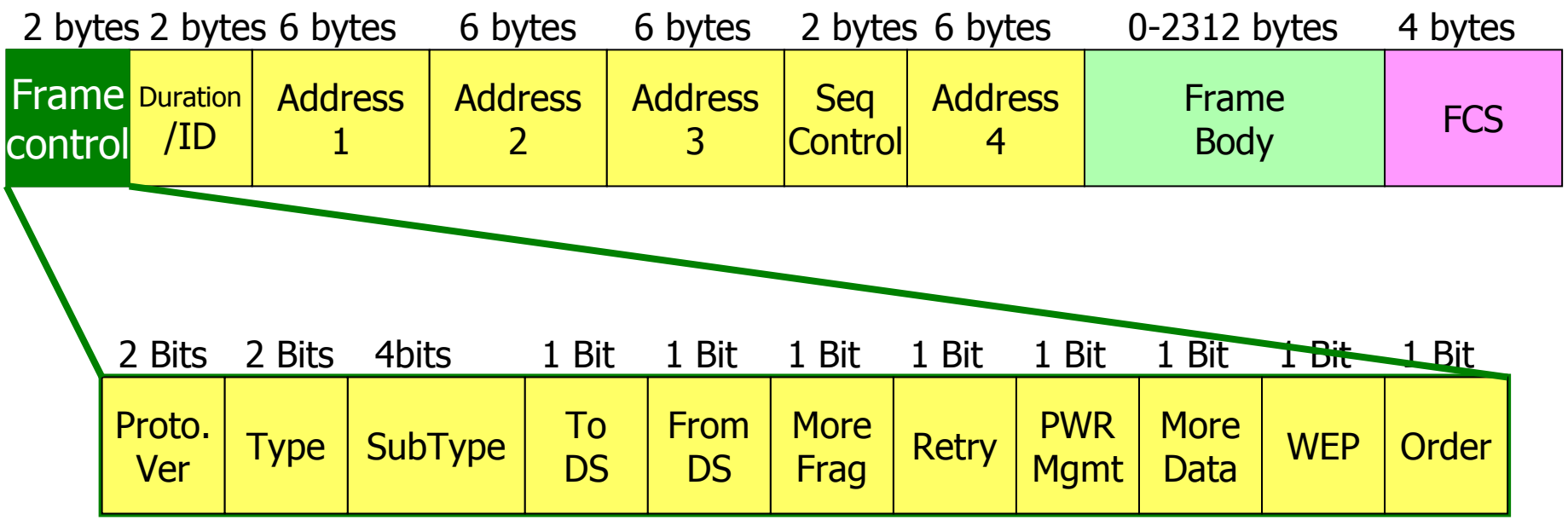
MAC Frame Structure



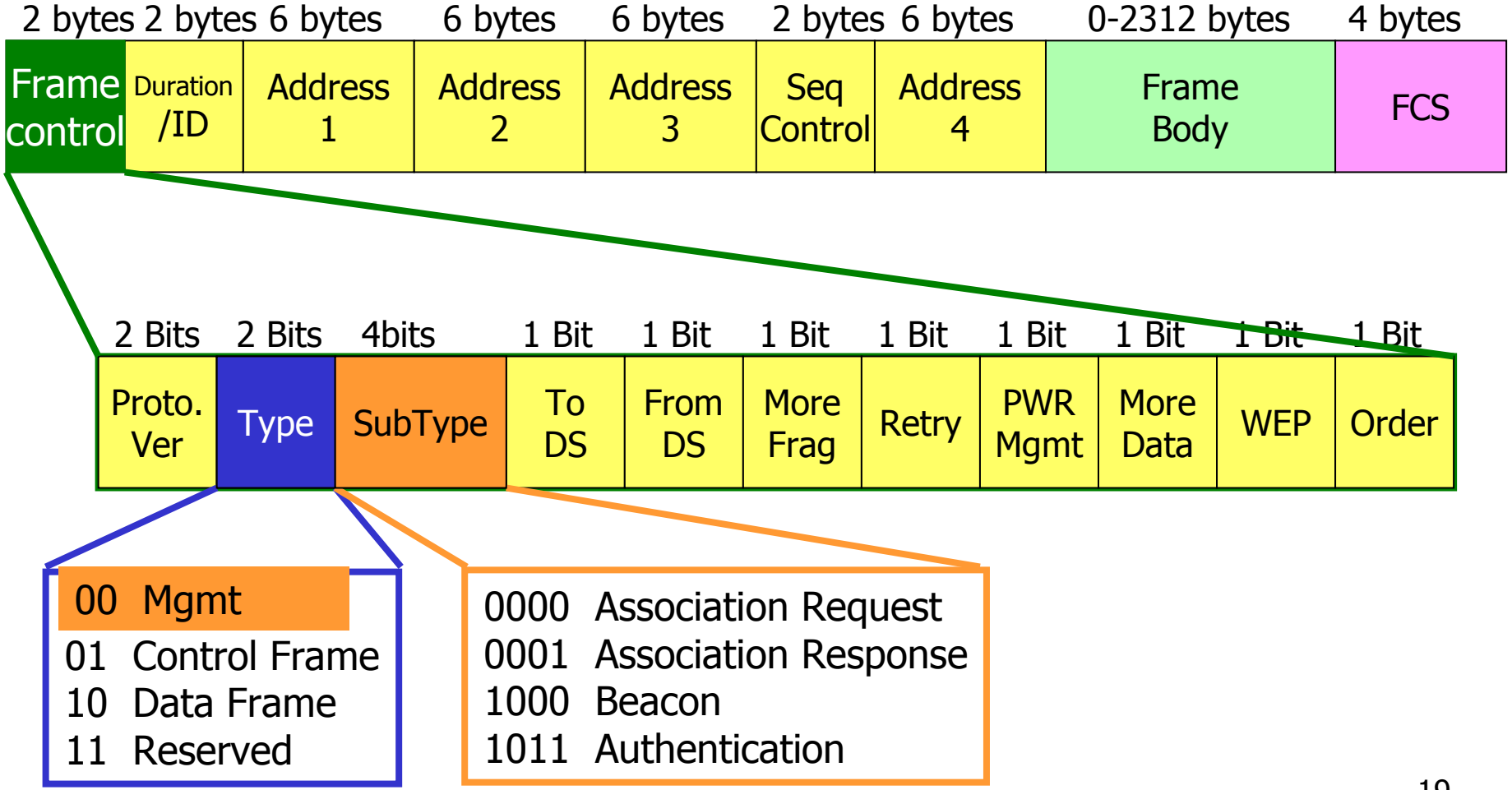
MAC Frame Structure



Frame Control Fields



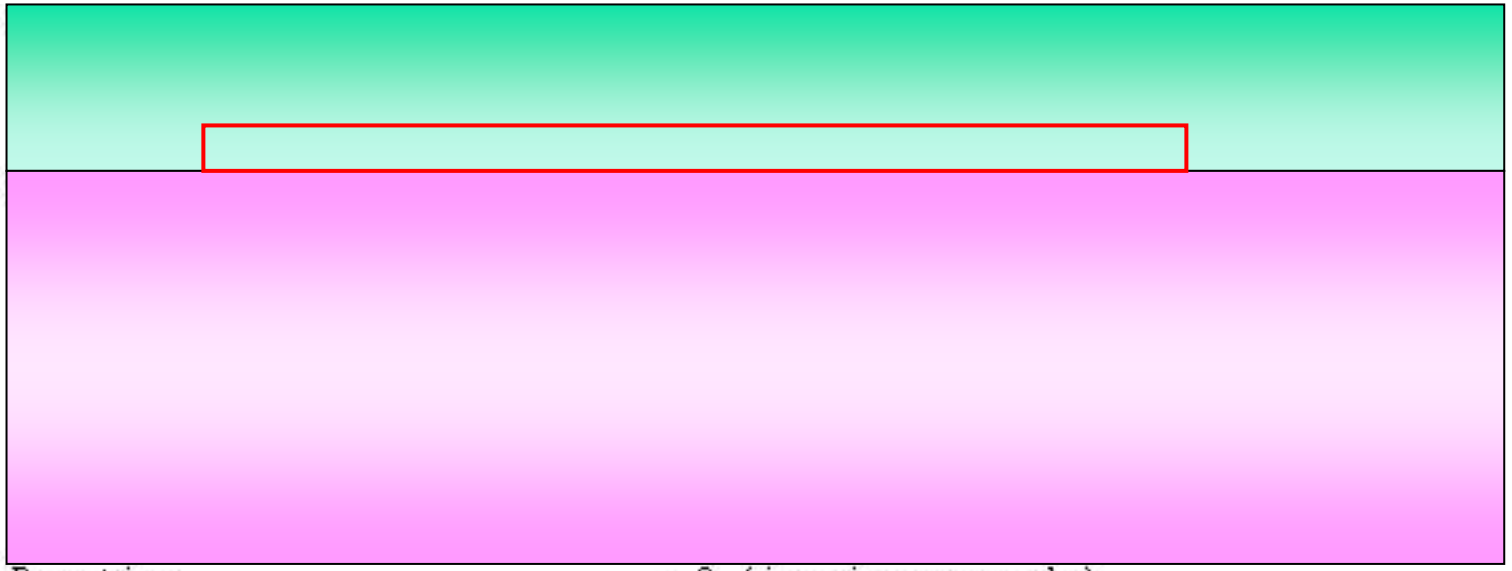
Frame Control – Type/subtype



Probe Request Frame

FC Byte#1

FC Byte#2



```
Duration                        = 0 (in microseconds)
Destination Address             = BROADCAST FFFFFFFFFFFF, Broadcast
Source Address                  = Station Aironт500292
Basic Service Set ID            = BROADCAST FFFFFFFFFFFF, Broadcast
Sequence Control                = 0x6F30
...Sequence Number              = 0x6F3 (1779)
...Fragment Number              = 0x0   (0)
Element ID                      = 0 (Service Set Identifier)
...Length                       = 7 octet(s)
...Service Set Identity         = "sliders"
```

http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.htm

Open Authentication Request

```
Frame 95 arrived at  10:49:47.8255; frame size is 30 (001E hex) bytes.
Signal level                    = 100%
Channel                         = 1
Data rate                       = 2 ( 1.0 Megabits per second)

Frame Control Field #1 = B0
             .... ..00 = 0x0 Protocol Version
             .... 00.. = 0x0 Management Frame
             1011 .... = 0xB Authentication (Subtype)
Frame Control Field #2 = 00
             .... ...0 = Not to Distribution System
             .... ..0. = Not from Distribution System
             .... .0.. = Last fragment
             .... 0... = Not retry
             ...0 .... = Active Mode
             ..0. .... = No more data
             .0.. .... = Wired Equivalent Privacy is off
             0... .... = Not ordered
Duration                        = 314 (in microseconds)
Destination Address             = Station Aironт31669C
Source Address                  = Station Aironт500292
Basic Service Set ID            = Aironт31669C
Sequence Control                = 0x0A40
...Sequence Number              = 0x0A4 (164)
...Fragment Number              = 0x0   (0)
Authentication algorithm number = 0 (Open System)
Authentication transaction sequence number = 1
Status code                     = 0 (Reserved)
```

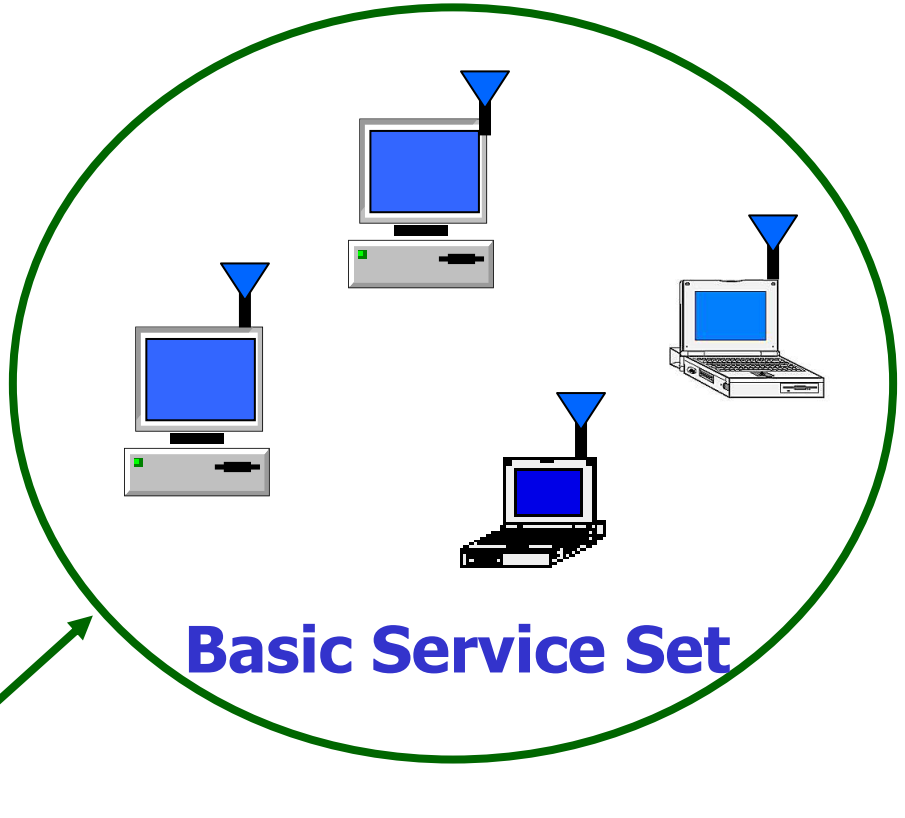
Open Authentication Request

(snap shot by Wireshark)

```
Frame 75 (54 bytes on wire, 54 bytes captured)
Radiotap Header v0, Length 24
IEEE 802.11 Authentication, Flags: ........
    Type/Subtype: Authentication (0x0b)
  Frame Control: 0x00B0 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 11
    Flags: 0x0
        DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    Duration: 44
    Destination address: Cisco_6f:f6:c0 (00:1e:f7:6f:f6:c0)
    Source address: IntelCor_39:42:4d (00:13:02:39:42:4d)
    BSS Id: Cisco_6f:f6:c0 (00:1e:f7:6f:f6:c0)
    Fragment number: 0
    Sequence number: 2204
IEEE 802.11 wireless LAN management frame
```

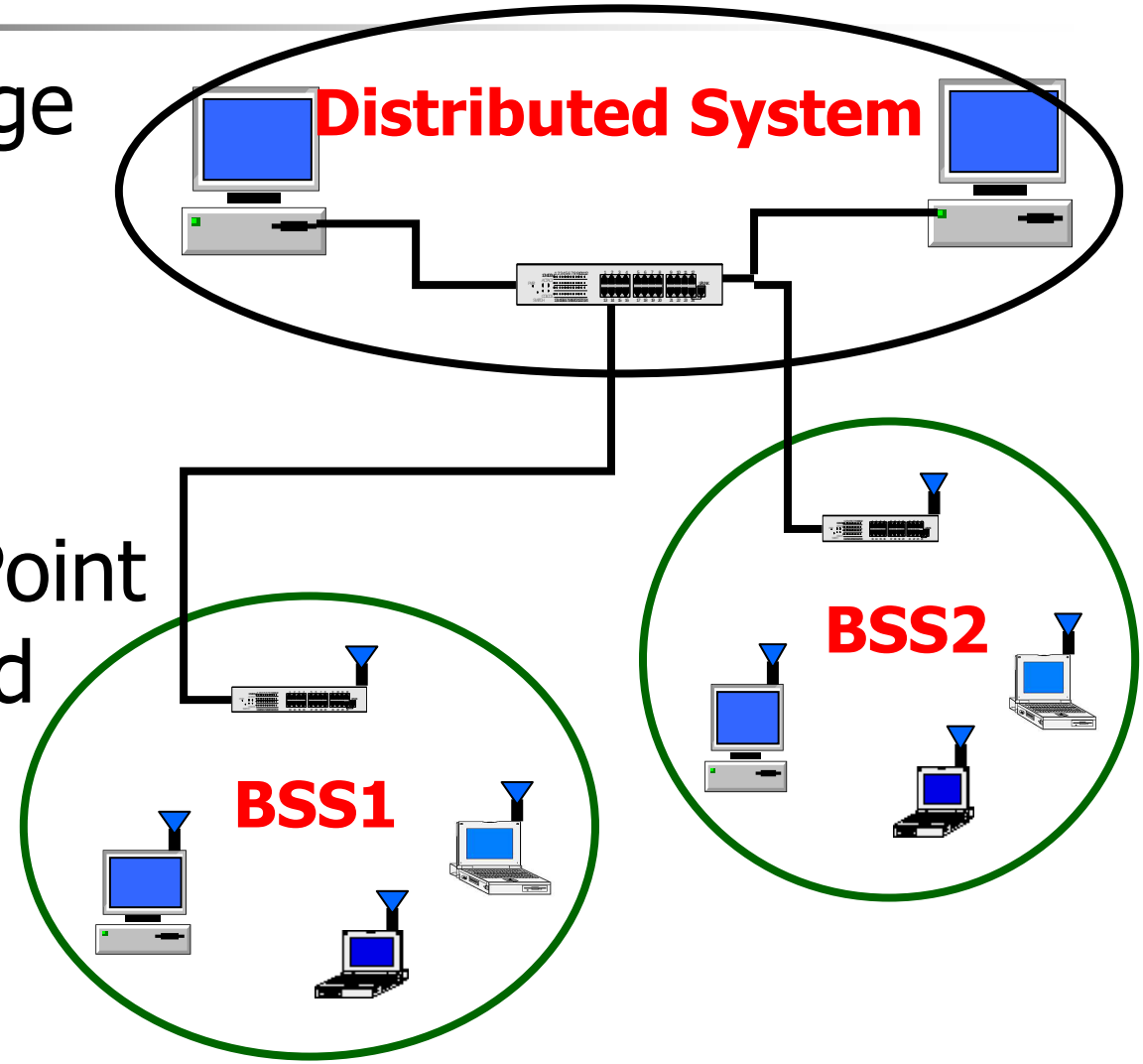
Independent Basic Service Set (IBSS)

- Stand-alone BSS
- No backbone infrastructure
- At least 2 stations
- **Ad hoc** Network
- Small area

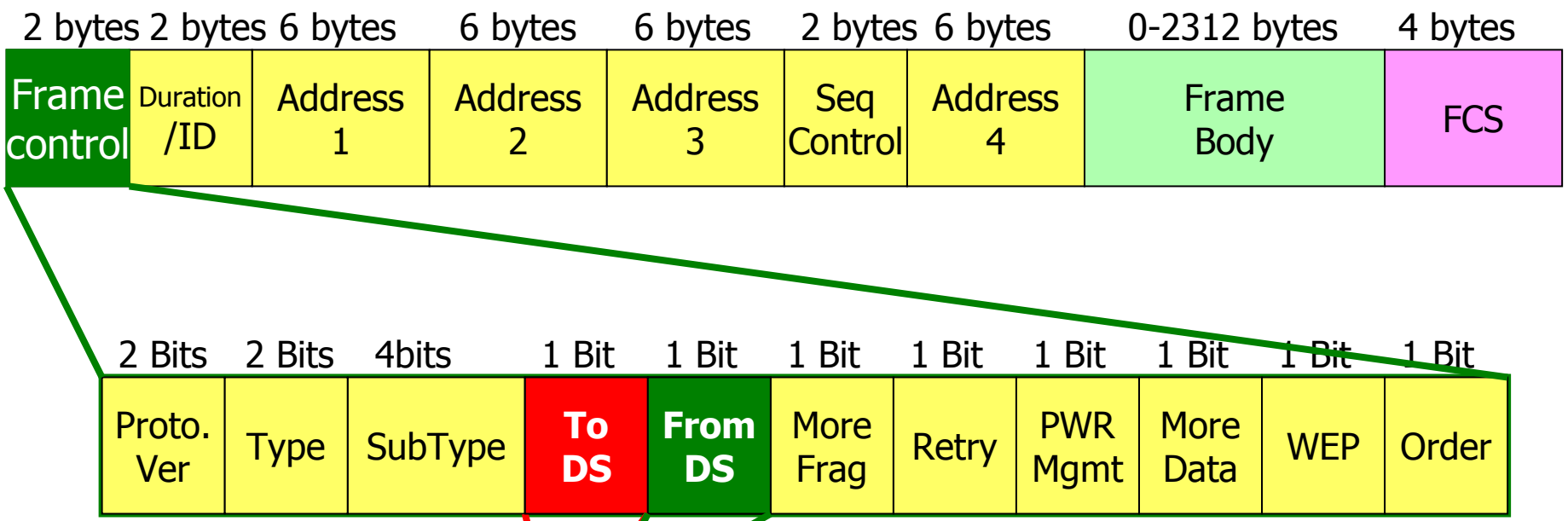


Extended Service Set (ESS)

- Extending range
- Arbitrary size
- Multiple cells interconnect
- Need Access Point and Distributed system



Frame Control – Address Fields



		Add 1	Add 2	Add 3	Add 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

DS: Distribution System

Address Example

```
Frame Control Field #1 = 40
                .... ..00 = 0x0 Protocol Version
                .... 00.. = 0x0 Management Frame
                0100 .... = 0x4 Probe request (Subtype)
Frame Control Field #2 = 00
```

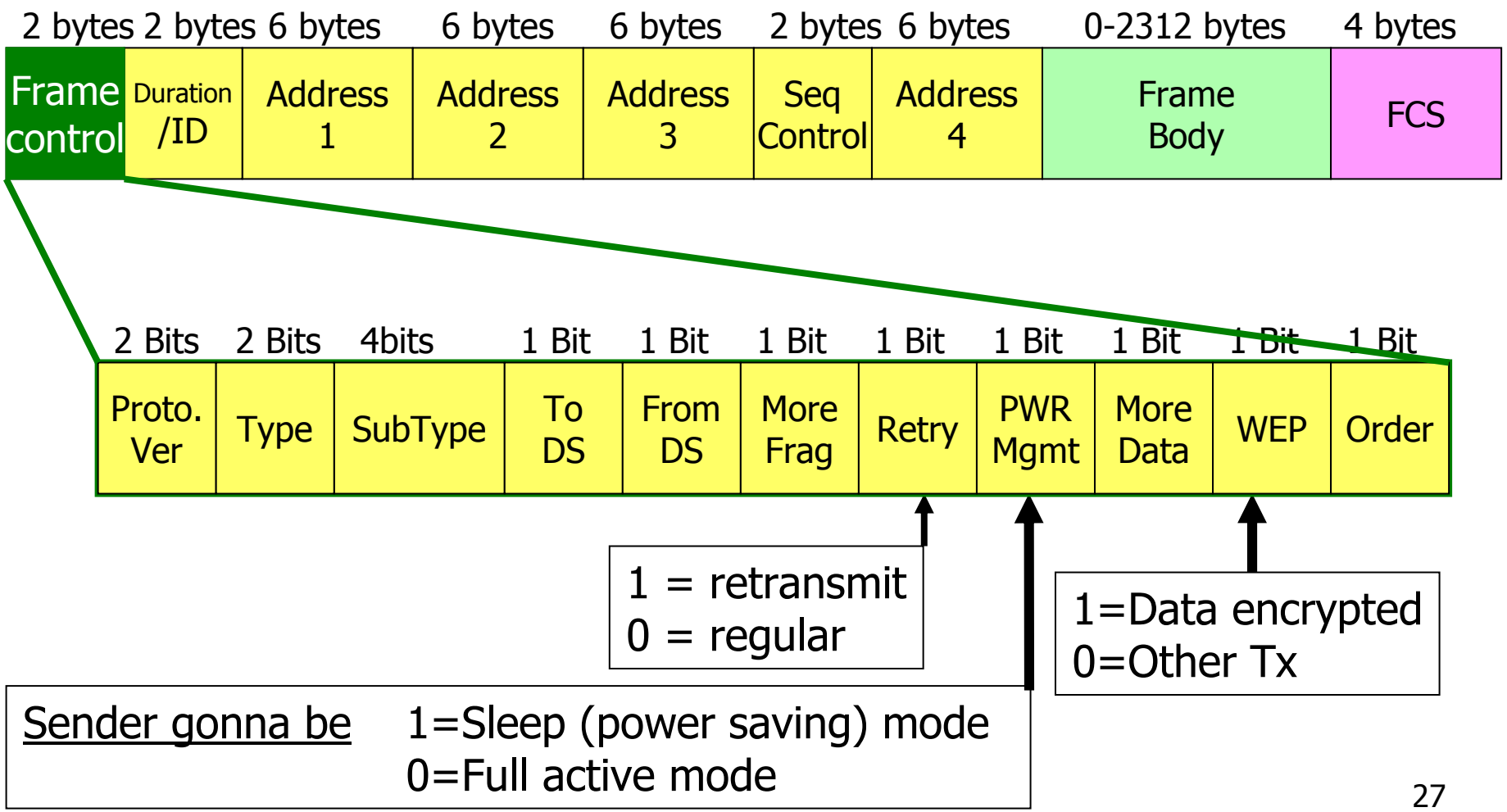
```
                .... .0.. = Last fragment
                .... 0... = Not retry
                ...0 .... = Active Mode
                ..0. .... = No more data
                .0.. .... = Wired Equivalent Privacy is off
                0... .... = Not ordered
Duration                  = 0 (in microseconds)
```

DA
SA
BSSID

```
Sequence Control          = 0x6F30
...Sequence Number        = 0x6F3 (1779)
...Fragment Number        = 0x0   (0)
```

http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.htm

Frame Control Fields



How to capture WLAN packets?

- To capture WLAN packet in Linux (Ubuntu)
  - Install Wireshark
    - `#sudo apt-get install wireshark`
  - Change your wireless NIC to “monitor” mode
    - Disable your WLAN card
      `# ifconfig wlan0 down`
    - Change mode of the wireless NIC card
      `# iwconfig wlan0 mode monitor`
    - Then up the interface
      `# ifconfig wlan0 up`
  - Now start the wireshark
- To stop capturing and start using the regular WLAN
  - Change mode of the wireless NIC card
    `# iwconfig wlan0 mode managed`

Capture packet
Live Demo

MAC Layer

- MAC Layer operation
  - Contention & contention-free
  - Priority frame transmission
- MAC frame structure/Types
  - MAC management, control, and data frame
- **Basic process revisit**

IEEE 802.11 Basic process

- Authentication
- Association
- Starting an IBSS
  - One station is configured to be “initiating station’’
  - Starter send beacons

Frame Control – Address Fields

To DS	From DS	Add 1	Add 2	Add 3	Add 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

00: All management/control frames
01: Data Frames from AP
10: Data Frames to AP
11: Data Frames on a wireless bridge

DS: Distribution System

DA: Destination Addr
SA: Source Addr
TA: Transmitter Addr
RA: Receiver Addr
BSSID: BSS ID same as AP

Traffic Flow

		Add 1	Add 2	Add 3	Add 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

MAC filters frames based on “Addr1”

- In IBSS:

  Traffic is sent directly to the destination in BSS

  Add1 = MAC add of the destination station

  Add2 = MAC add of the source station

  Add3 = BSSID (= MAC add of the initiator of the IBSS)

- In ESS:

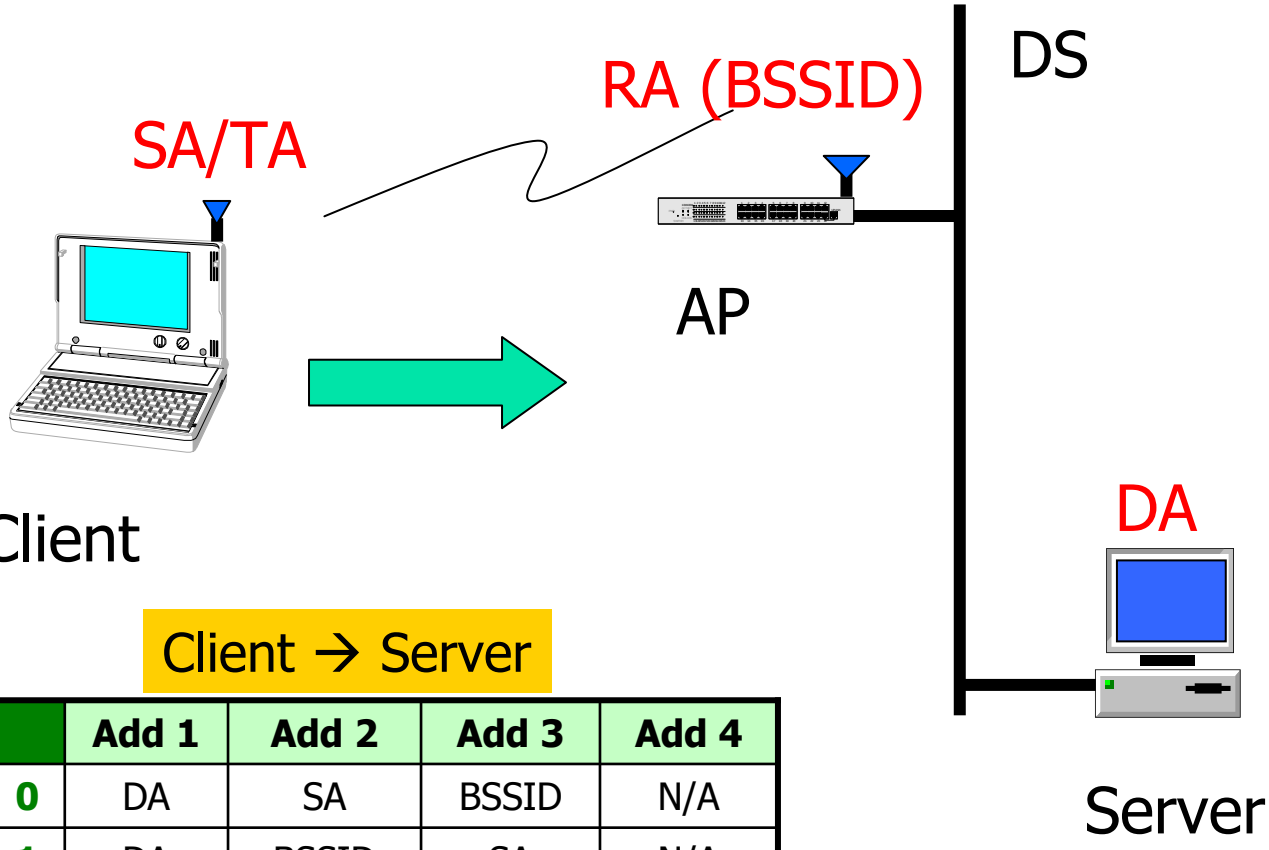
  Outgoing traffic is sent to Access-Point in BSS

  Add1 = MAC add of the Access-Point

  Add2 = MAC add of the source station

  Add3 = MAC add of the destination station

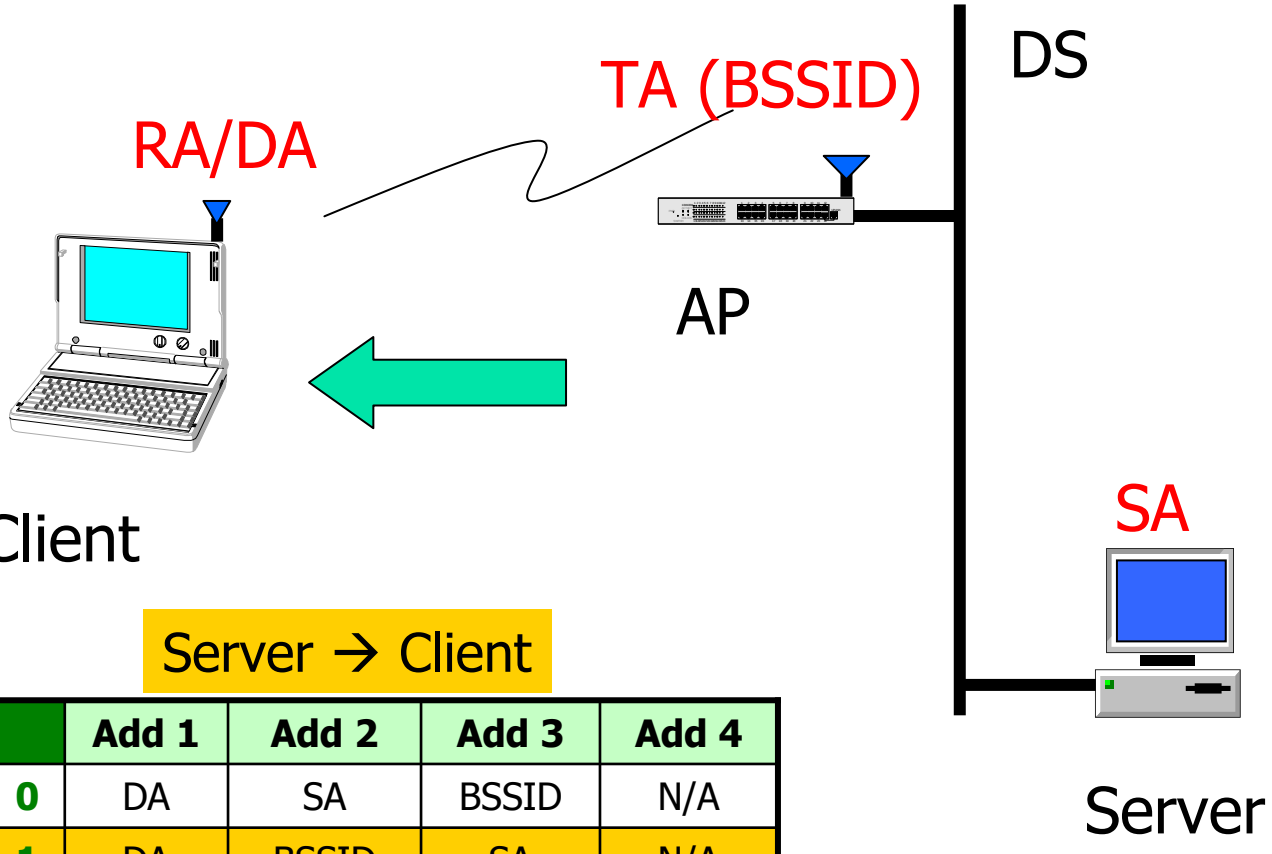
Address Fields (To AP)



Client → Server

		Add 1	Add 2	Add 3	Add 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

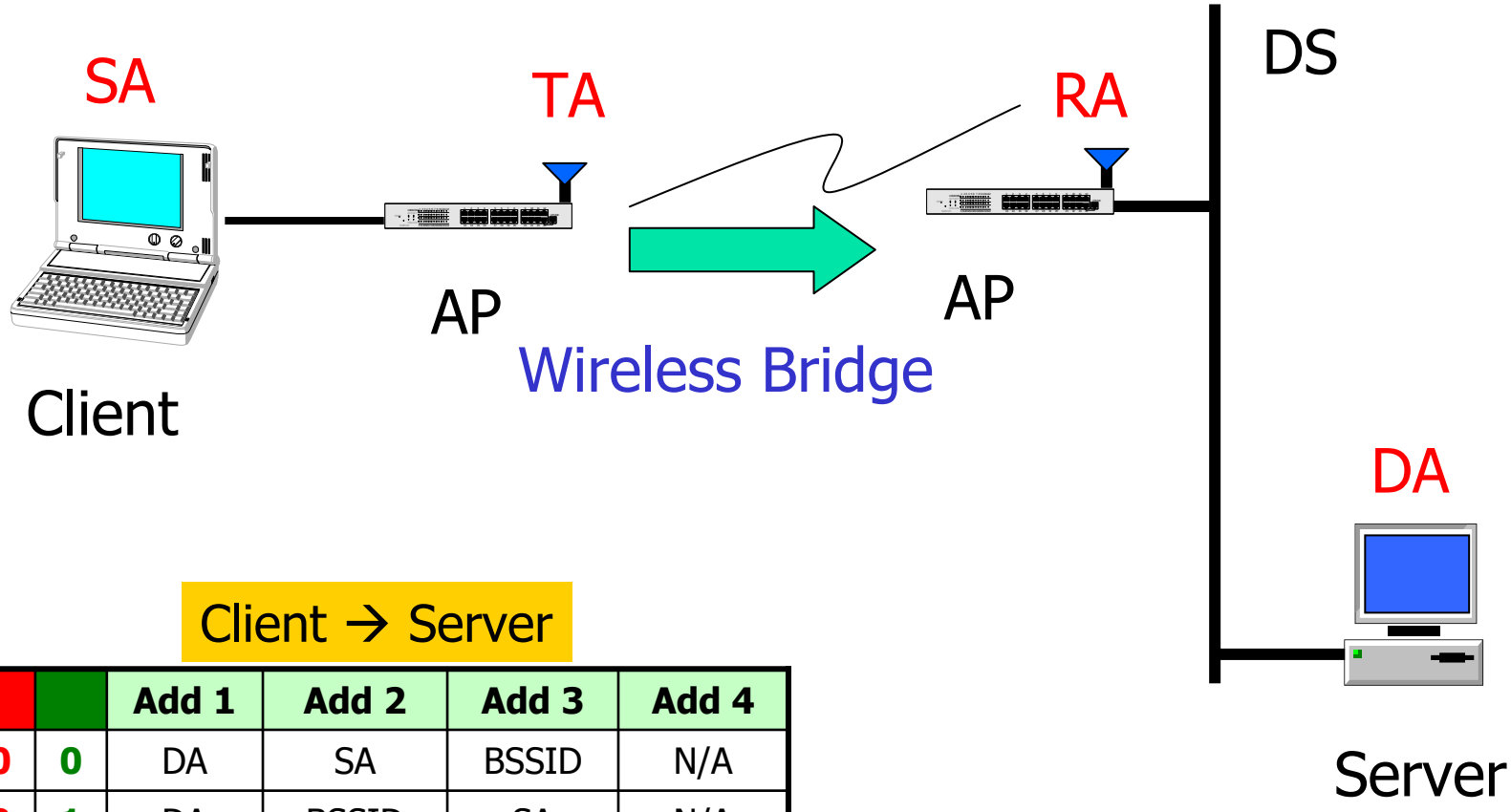
Address Fields (From AP)



Server → Client

		Add 1	Add 2	Add 3	Add 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

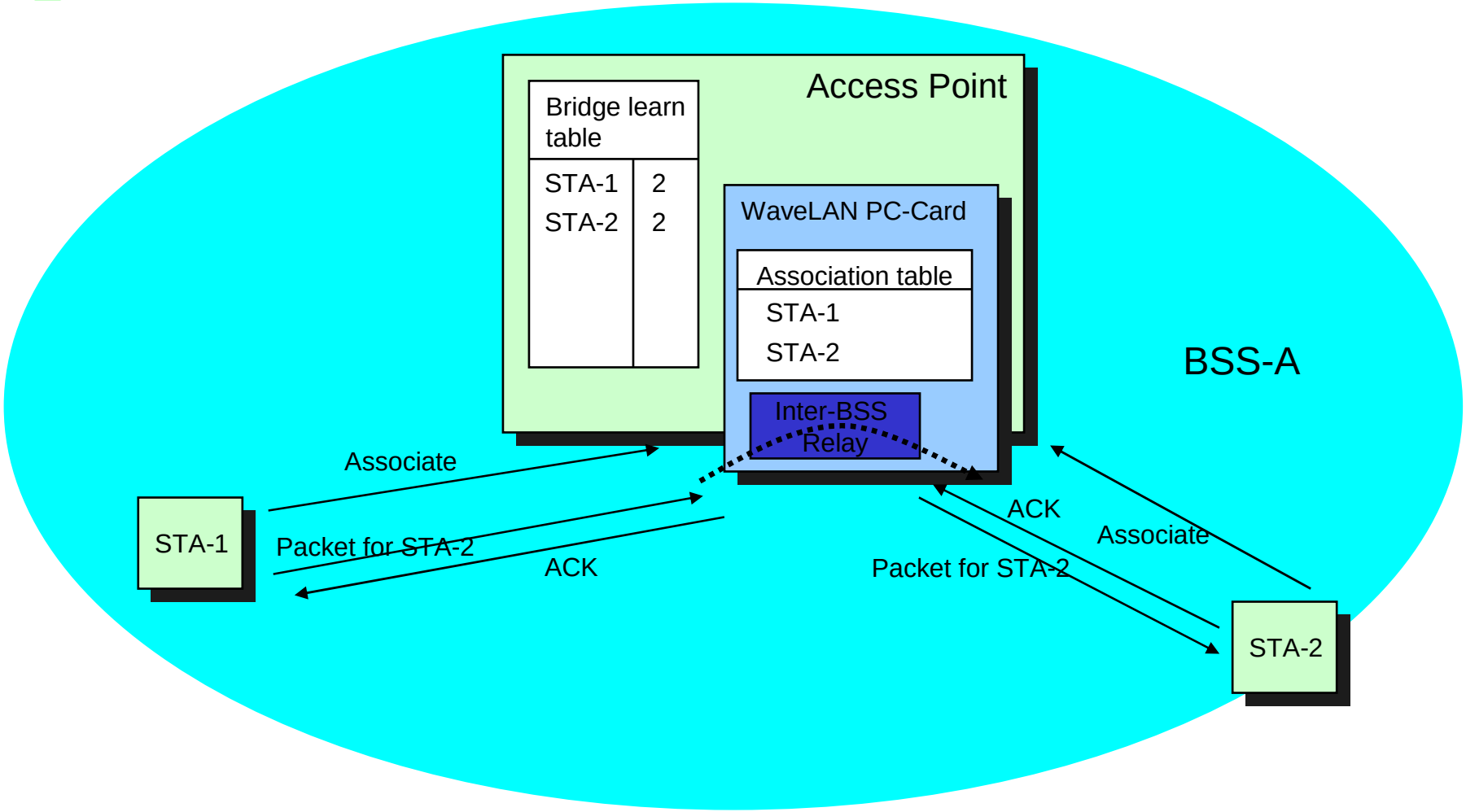
Address Fields (WDS)



Client → Server

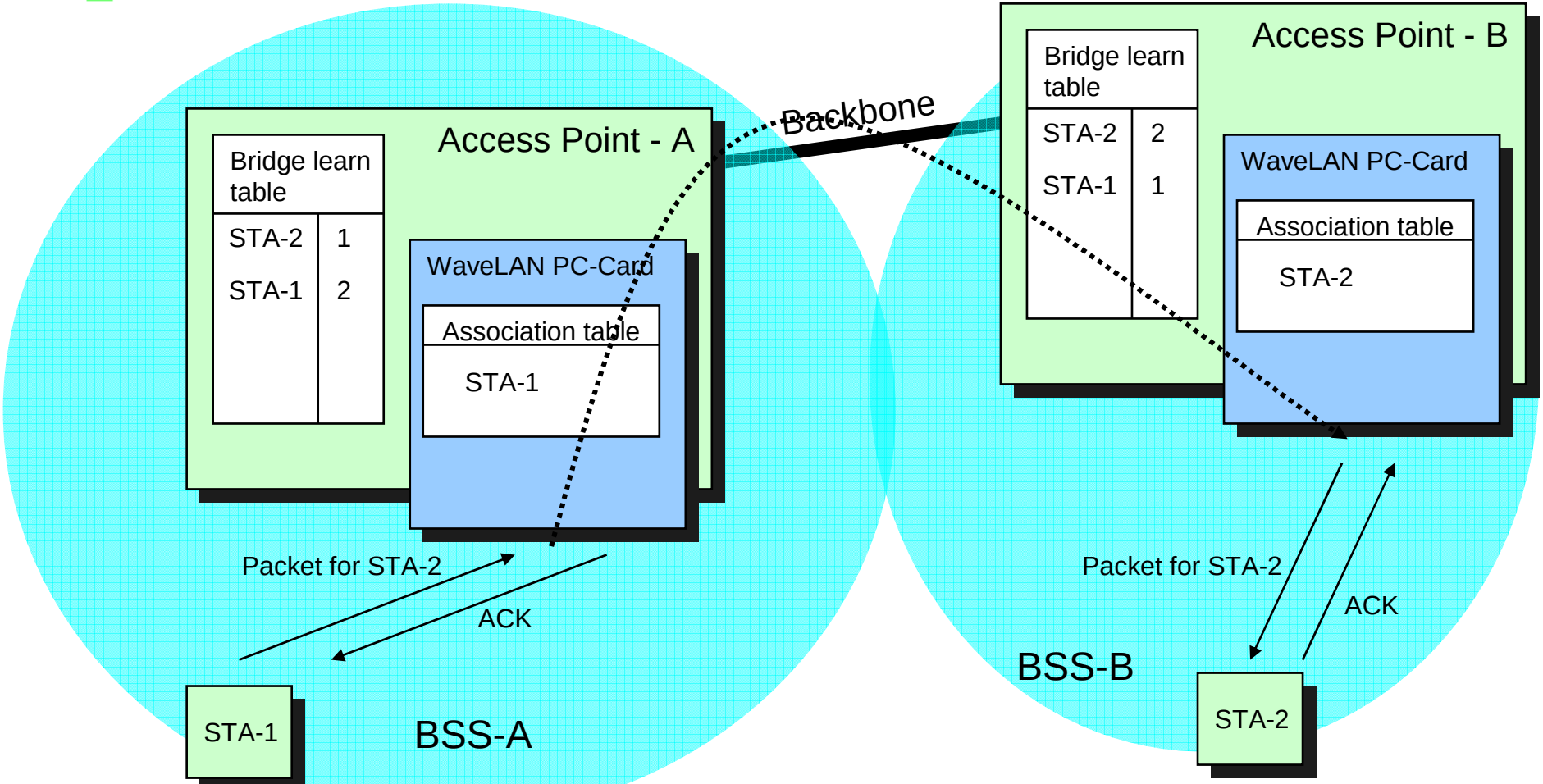
		Add 1	Add 2	Add 3	Add 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Traffic flow inside BSS



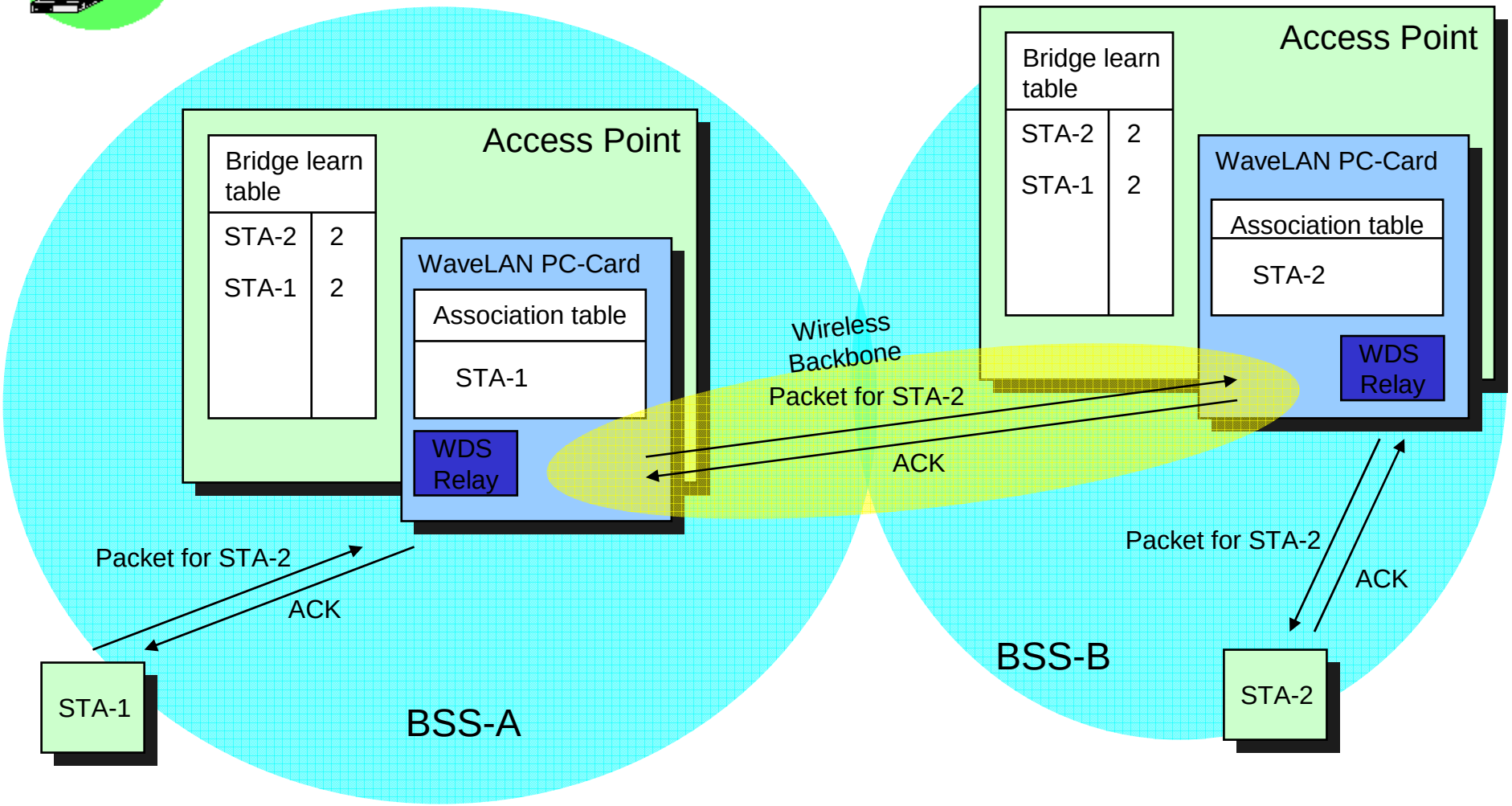
From WaveLAN Slide

Traffic flow in ESS



From WaveLAN Slide

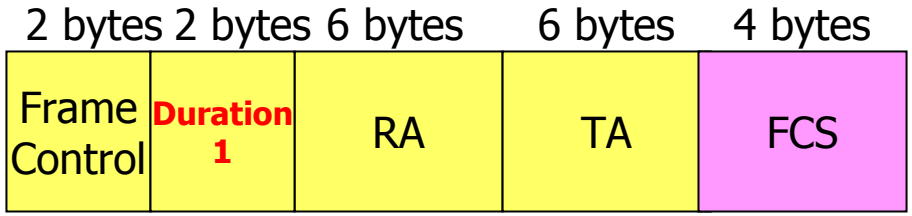
Traffic flow in WDS

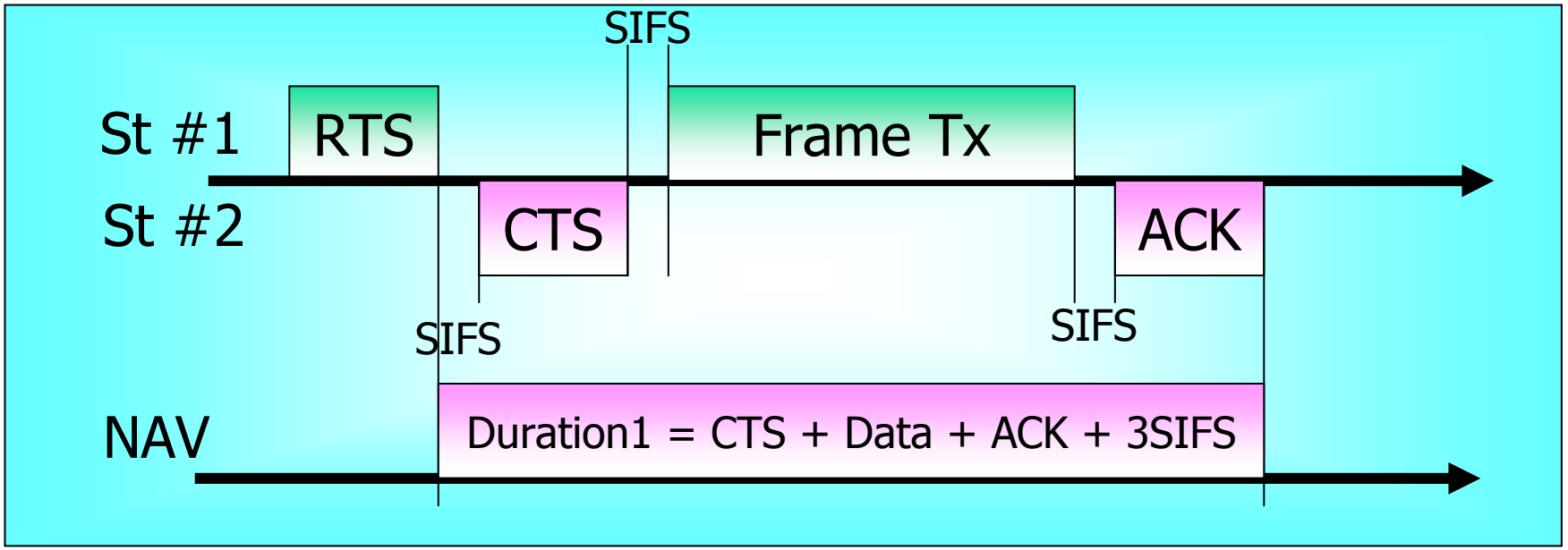


From WaveLAN Slide

Control Frame : RTS

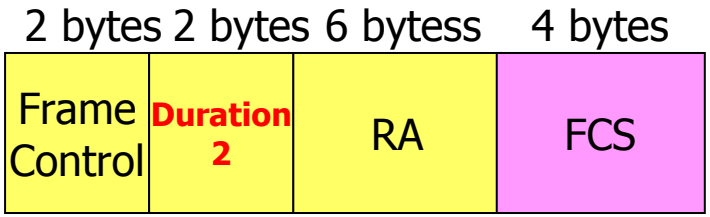
RTS frame

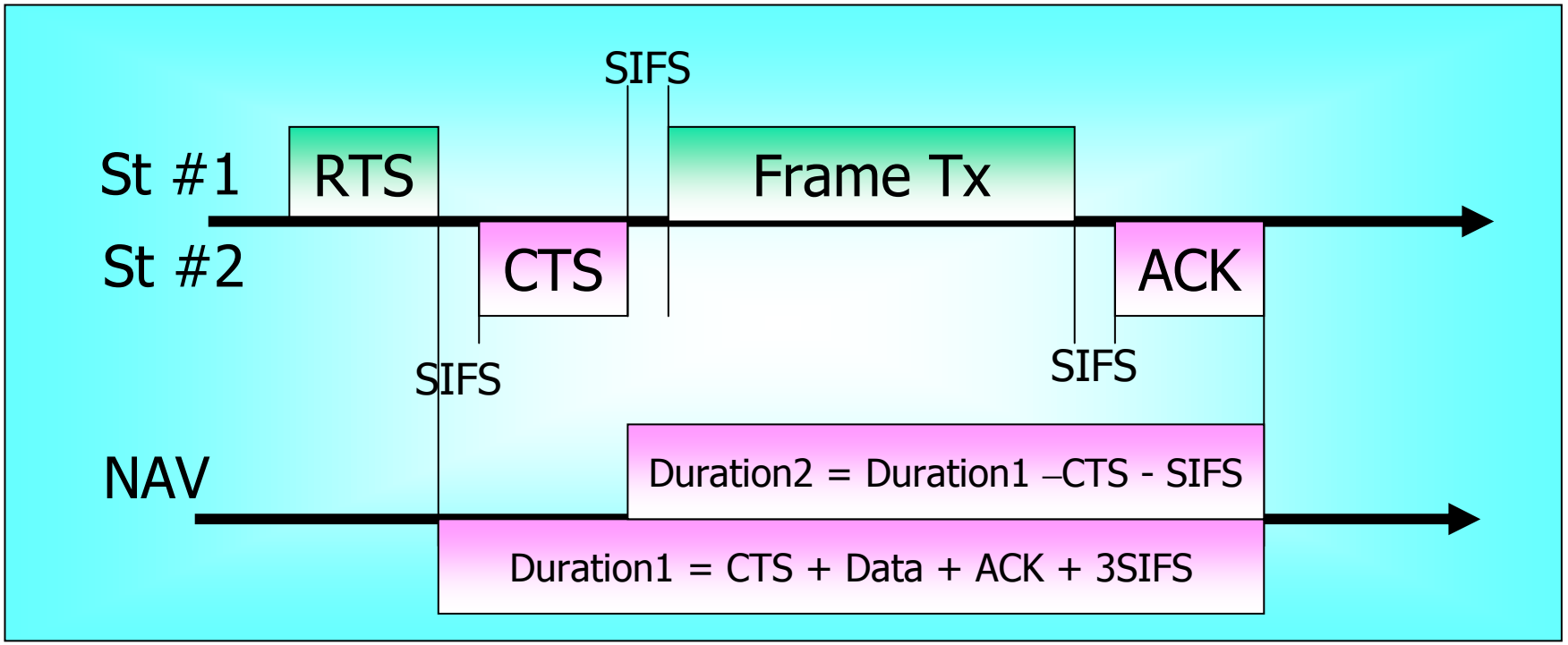




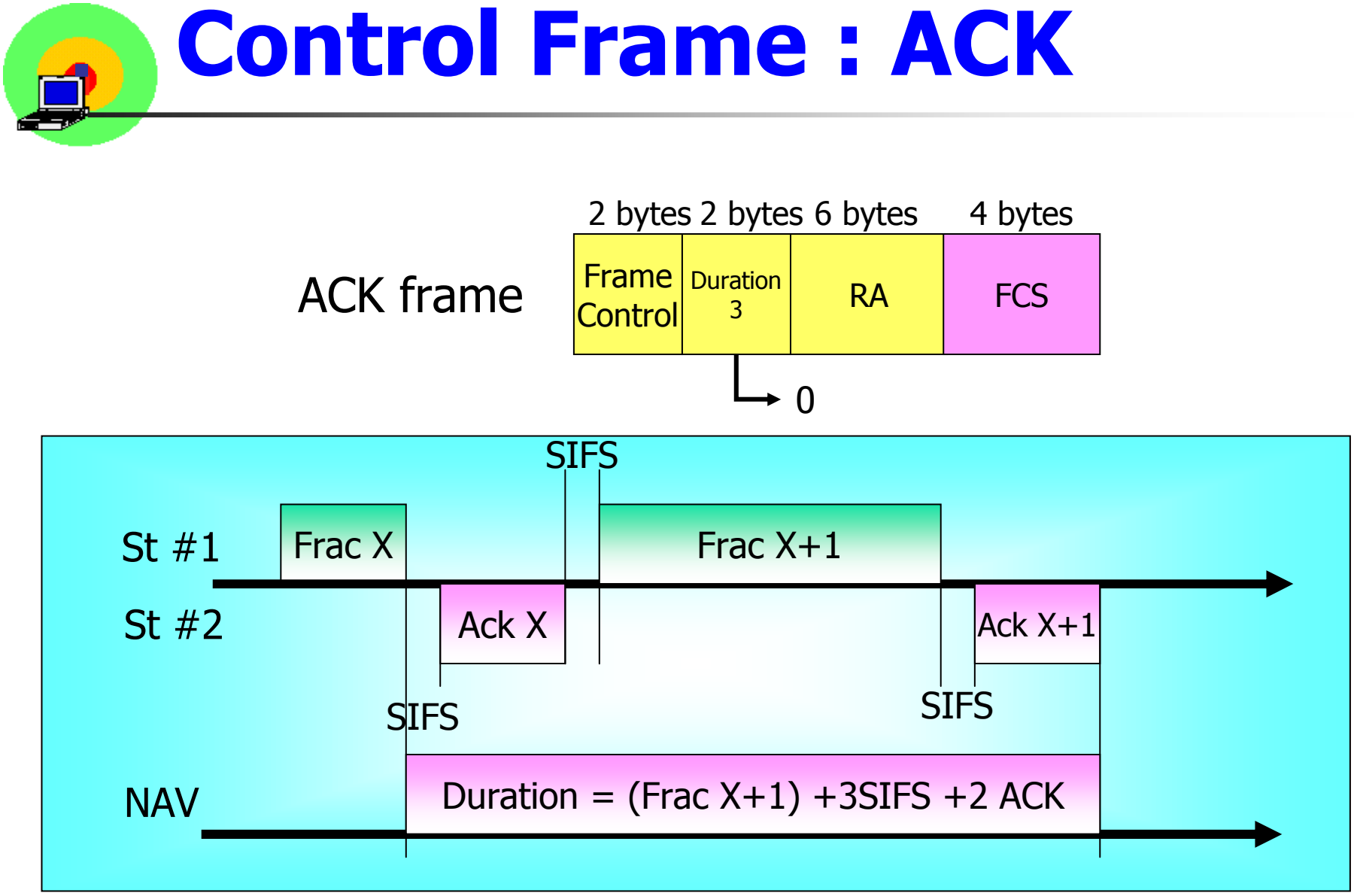
Control Frame : CTS

CTS frame





Control Frame : ACK



Management Frame: Beacon

- Announce the existence of a network
- Regular intervals
- Allow network management
- AP is responsible

Beacon Frame

```
▷ Frame 14 (192 bytes on wire, 192 bytes captured)
▷ Radiotap Header v0, Length 24
▽ IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x08)
  ▽ Frame Control: 0x0080 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 8
    ▽ Flags: 0x0
        DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Cisco_6f:f6:c0 (00:1e:f7:6f:f6:c0)
    BSS Id: Cisco_6f:f6:c0 (00:1e:f7:6f:f6:c0)
    Fragment number: 0
    Sequence number: 3932
▷ IEEE 802.11 wireless LAN management frame
```

Power Conservation

- Mobility relies on **batteries**
- Frequently recharge is undesirable
- How to save the battery ??
  - Power down the transceiver
- Power down status
  - Sleep/Doze/Power saving mode
- Power up status
  - Active/Awake mode

Power Saving Goal

- Minimizing time spent in the Awake mode
- No scarify for network connectivity

Power conservation
in the Infrastructure Mode

- All traffic go through Access Point
- AP is always active (connected to power supply)
- (Associated) Mobile nodes send their status to AP
- AP manages timing for sending data
  - AP sends data to the active node
  - Periodically announce to sleep nodes if data is waiting (Keep buffering the data)

Power consumption

Mode	Power Consumption
Awake – Transmit packets	1.65 W *1
Awake – Receive packets	1.40 W *1
Awake – Idle	1.15 W *1
Doze	0.045 W *2

*1Mark Stemm and Randy H. Katz, “Measuring and reducing energy consumption of network interfaces in hand-held devices,” IEICE Transactions on Communications, special Issue on Mobile Computing, vol. E80-B, no. 8, pp. 1125–31, 1997

*2Havinga P.J.M., Smit G.J.M., “Energy-efficient TDMA medium access control protocol scheduling”, Asian International Mobile Computing Conference (AMOC 2000), Nov. 2000.

Power saving

- Doze mode
  - Default state
  - keep radio off most of the time
  - wakeup periodically to check for message
- Sleep mode
  - radio in transmit-only standby mode
  - radio wake up and send if necessary but cannot receive

Sleep time

- Negotiate in the association process
- "**Listen Interval**" parameter (#beacon periods)
- Long interval ➔ large buffer needed @AP
- Time up ➔ AP discards buffered frames

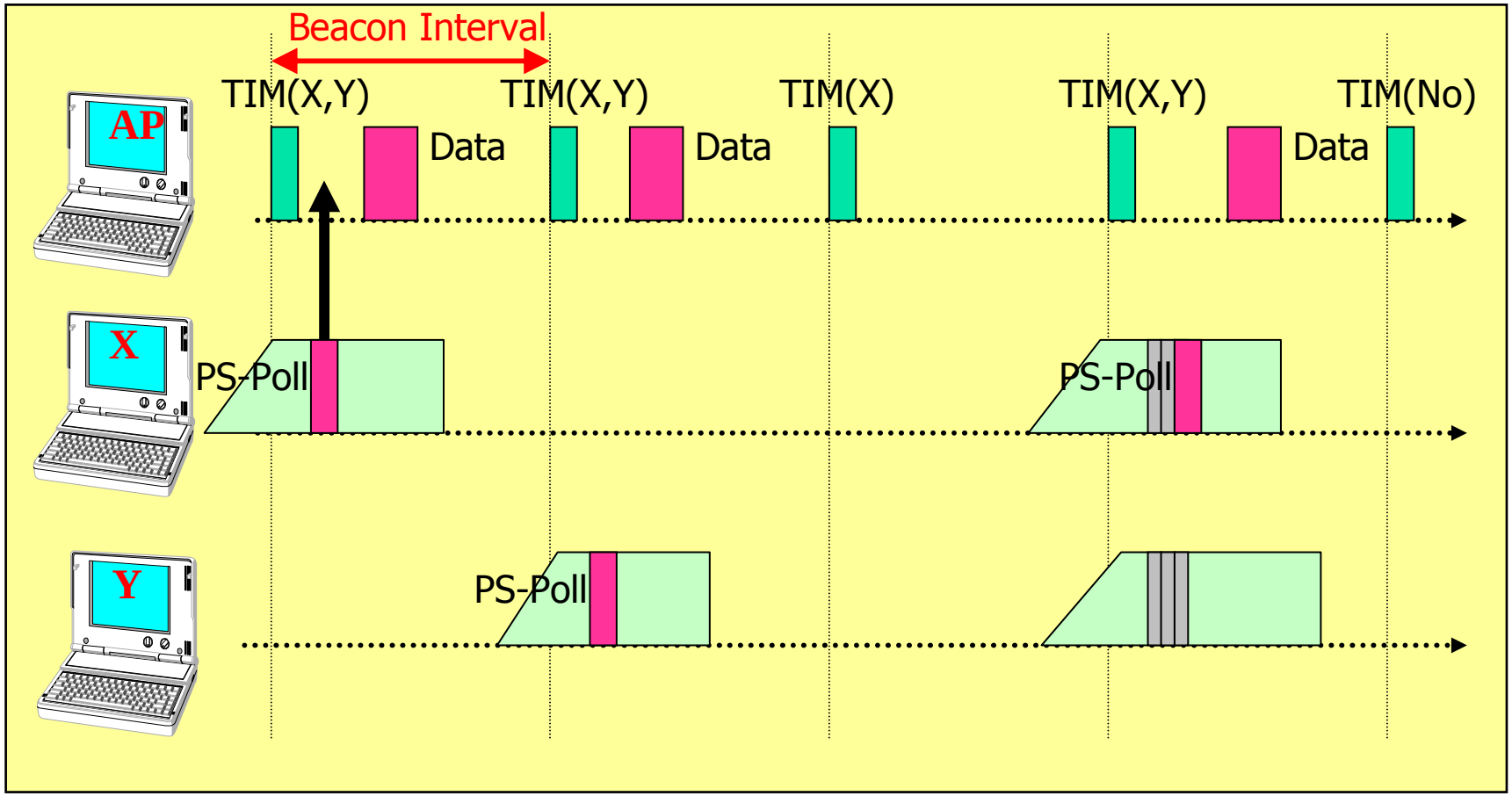
Management Frame: TIM

- Traffic Indication Map
- Low-power mode
- TIM is transmitted in the Beacon frame
- AP sends to sleeping station (data is waiting for the sleeping station)
- Each node must wake up to listen for Beacon frame (with TIM included)

Traffic Indication Map (TIM)

- A virtual bitmap
  - Each bit for each Association ID (AID)
  - “Set” bit = AP has buffered unicast frames for the AID station
  - Size = 2008 bits

Frame Retrieval Process



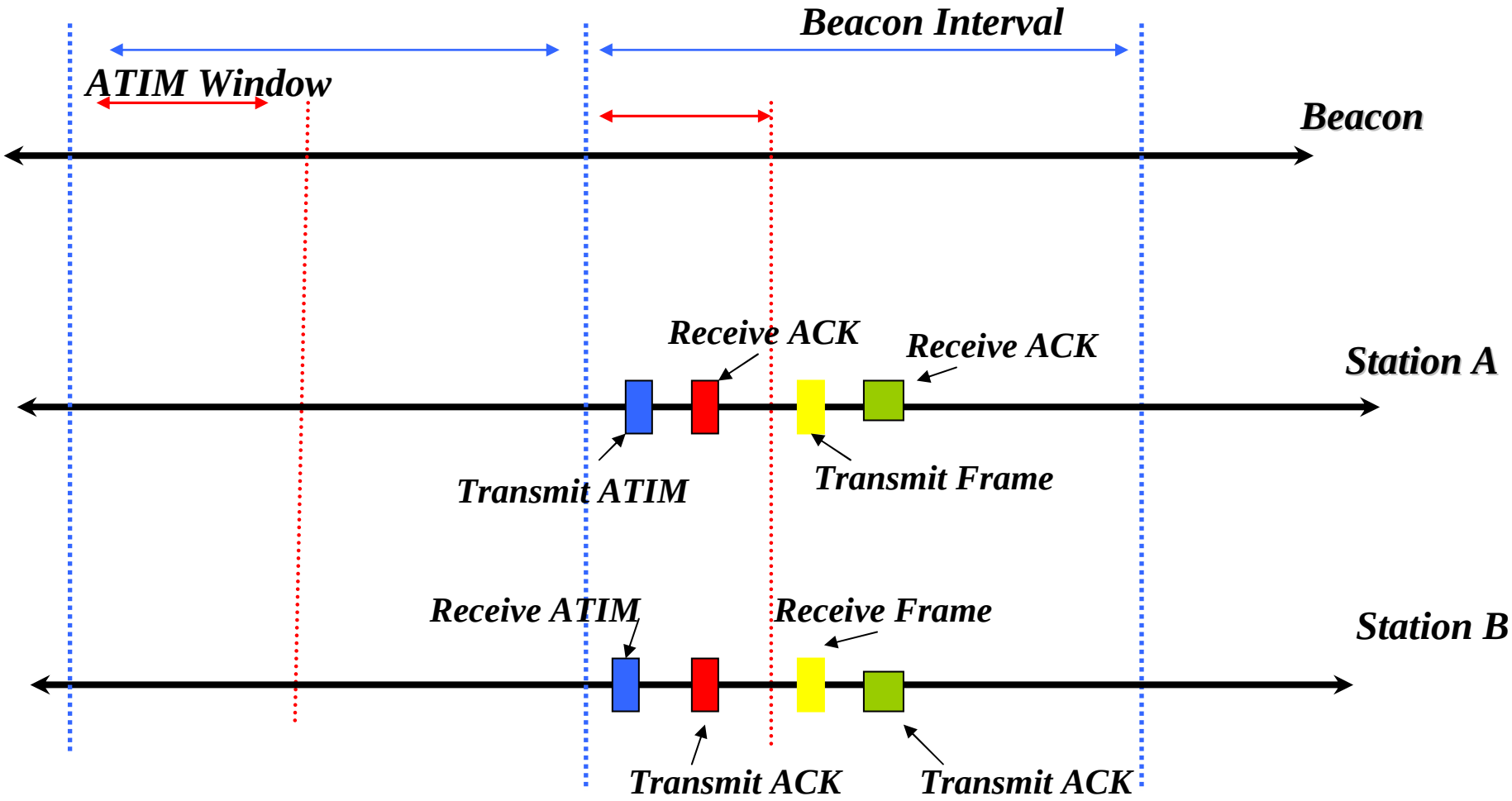
PS = power saving

X: listen interval = 3
Y: listen interval =2

Other TIM

- Delivery TIM (DTIM)
  - Multicast and Broadcast frames
- ATIM (Announcement TIM)
  - used in IBSS Beacon Frame
  - # of time units between ATIM frames

Power Management in IBSS



More Data

- Mobile node sends a PS-Poll for a buffered frame
- AP sends back data
- Observed the “More Data” bit in Frame Control
- Sending more PS-Poll if More Data ≠ 0