جامعة الأهرام الكندية
AHRAM CANADIAN UNIVERSITY

Lecture (08)
Wireless Traffic Flow and AP Discovery

Dr. Ahmed ElShafee

Agenda

- Wireless Frame Types
- Sending a Frames
- Wireless Frame Headers
- Frame Types
- A Wireless Connection, the whole story

Wireless Frame Types

Wireless LANs come in three frame types:

- **Management frames:**
  Used for joining and leaving a wireless cell.
  Management frame types include association request, association response, and re-association request,
- **Control frames:**
  Used to acknowledge when data frames are received.
- **Data frames:**
  Frames that contain data.

Sending a Frame

- Wireless networks are half-duplex networks.
- If more than one device were to send at the same time, a collision would result.
- If a collision occurs, the data from both senders would be unreadable and would need to be resent.
- This is a waste of time and resources.
- To overcome this issue, wireless LANs use carrier sense multiple access collision avoidance (CSMA/CA),
- Which is similar (some how) to the way 802.3 LANs work.

- The *carrier sense part means that a station* has to determine if anyone else is sending.
- This is done with clear channel assessment (CCA), and what it means is that you listen.

Inter-frame space

- As a part of collision avoidance, Each station must also observe IFS.
- IFS is a period that a station has to wait before it can send.
- Not only does IFS ensure that the medium is clear, but it ensures that frames are not sent so close together that they are misinterpreted.

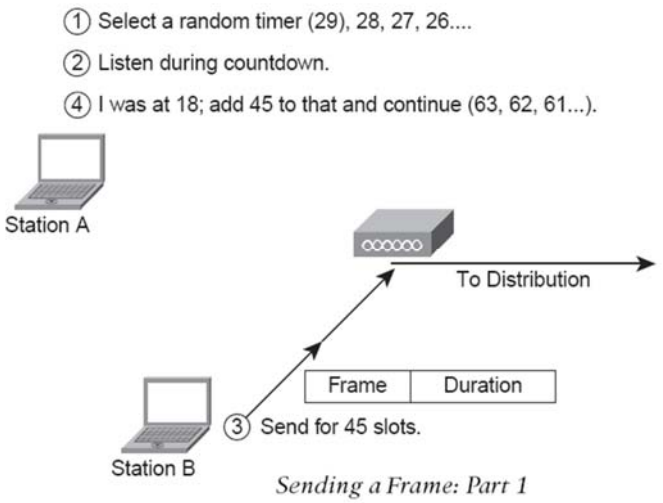
The types of IFS periods

- **Short interframe space (SIFS):**
  - For higher priority and used for ACKs, among other things
  - SIFS is used when you must send a frame quickly.
  - For example, when a data frame is sent and must be acknowledged (ACK), the ACK should be sent before another station sends other data.

- **Point-coordination inter-frame space (PIFS):** Used when an AP is going to control the network
- **Distributed-coordination inter-frame space (DIFS):**
  - Used for data frames and is the normal spacing between frames.
  - Data frames use DIFS.
  - The time value of DIFS is longer than SIFS, so the SIFS would preempt DIFS because it has a higher priority.

Frame transmission process

- Station A wants to send a frame.
- Client listens to physical carrier to ensure it's free.
- To listen, the client chooses a random number and begins a countdown process, called a *back-off timer*
- The speed at which the countdown occurs is called a ***slot-time*** *and is different for 802.11a, b, and g.*



Sending a Frame: Part 1

It works like this:

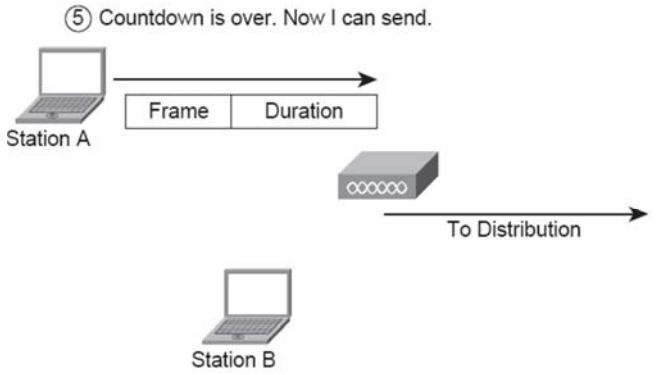
1. Station A selects the random timer value of 29.
2. Station A starts counting at 29, 28, 27, 26, and so on.
3. While Station A is counting down, it is also listening for whether anyone else is sending a frame.
4. When the timer is at 18, Station B sends a frame, having a duration value in the header of 45.
5. The duration of 45 that is in the header of the frame sent by Station B is called **a *network allocation vector (NAV)*** *and is a reservation of the medium that includes* the amount of time to send its frame, wait for the SIFS, and then receive an ACK from the AP.

6. Station A adds 45 to the 18 that is left and continues counting down, 63, 62, 61, and so on.

   The total time that Station A waits before sending is called the ***contention window***.

6. After the timer on Station A reaches 0, it can send its frame as illustrated in Figure.

   At this point, the medium should be clear.



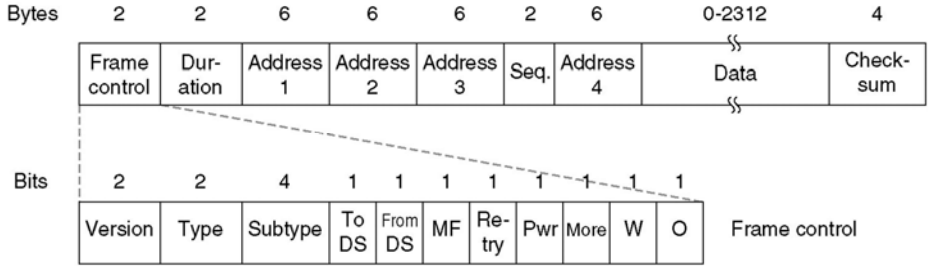
Sending a Frame: Part 2

- If Station A sends but fails, it resets the back-off timer to a new random number and counts down again.
- The back-off timer gets larger as the frames fail in transmission.
- For example, the initial timer can be any number between 0 and 31.
- After the first failure, it jumps to any number between 0 and 127.
- It multiplied by 4 for the next failure, then again, then again.

- This entire process is known as the ***distributed coordination function (DCF).***
- *This simply* means that each station is responsible for coordinating the sending of its data.
- The alternative to DCF is ***point coordination function (PCF),*** *which means the AP is responsible for* coordination of data transmission.

- If the frame is successful, an ACK must be sent.
- The ACK uses the SIFS timer value to make sure it is sent quickly.
- Some amount of silence between frames is natural.
- The SIFS is the shortest period of silence.

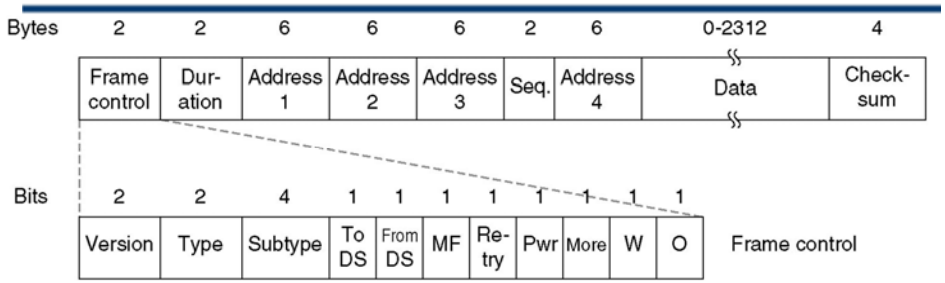
Wireless Frame Headers



- Starts with **preamble**, which can be anywhere from 76 to 156 bytes.
- The **Frame Control field** is 2 bytes.
- Contains protocol version (2bits), frame type (2bits)/subtype (4bits), and 8 flags

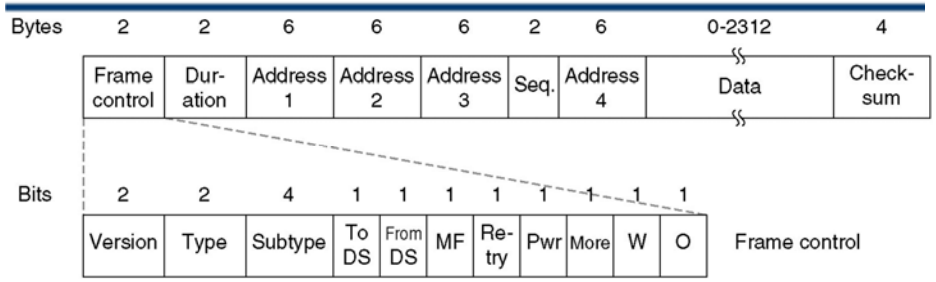
- The Flags field indicates that the frame is traveling *from the DS, not toward the DS (distributed system).*

```
▽ Flags: 0xA
    DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x02)
    .... .0.. = More Fragments: This is the last fragment
    .... 1... = Retry: Frame is 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
```

- The Duration field indicates how long the medium is reserved while this frame is being sent and includes time for an ACK to be sent in reply.

  The idea behind this process is to prevent collisions.

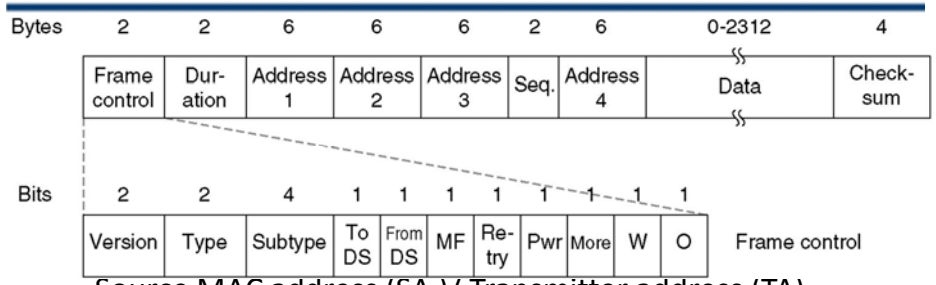


- A wireless frame can have up to three MAC addresses following the Duration field.

  This is a total of 18 bytes.

  – Source address

  – Destination address

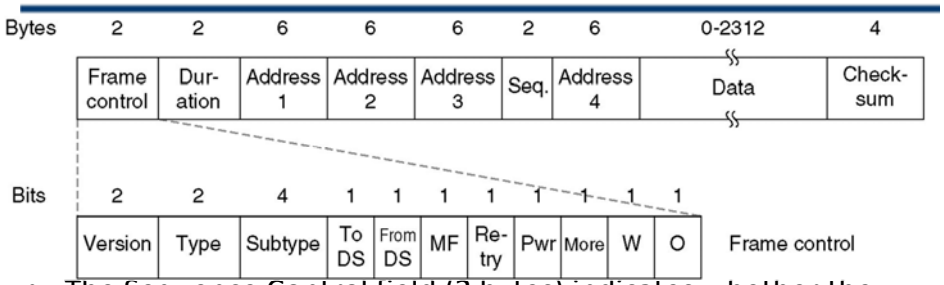


  – Source MAC address (SA)/ Transmitter address (TA)

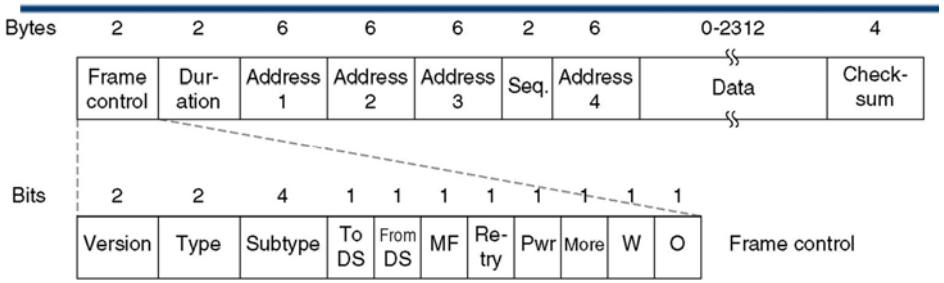
    SA is the station that sent the frame, while TA is the address of the station that is emitting the frame

  – In some scenarios, a TA might vary from an SA.

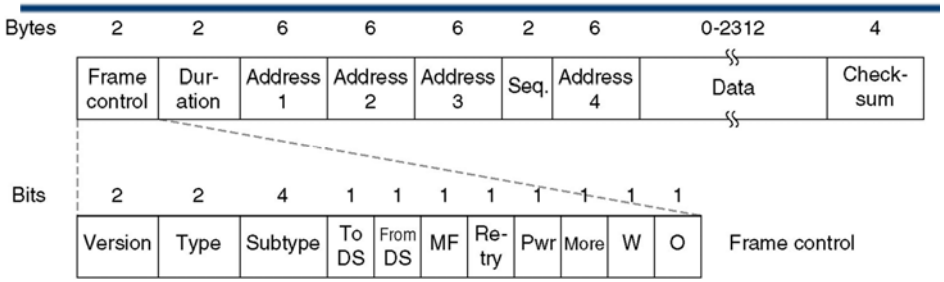
  – For example, if a wireless frame is relayed through a repeater, the TA would be the radio of the repeater, and the SA would be the sending device.



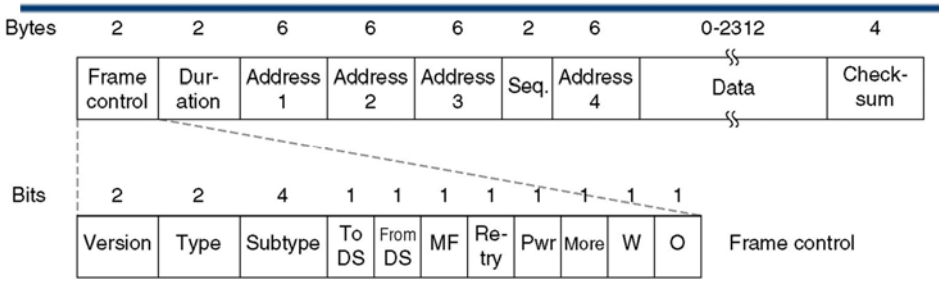
- The Sequence Control field (2 bytes) indicates whether the frame is a fragment.
  - the Sequence Control field is indicated with *Fragment Number*
  - *Wireless frame length* by default, 2346 bytes.
  - While Ethernet has a maximum transmission unit (MTU) of 1500 bytes



  - Fragmentation is needed if frame is going to move to or from an Ethernet distribution, the frames on the wireless side are too big and need to be chopped up.



- (4th address)Receiving address (RA)**:** which is the address of the *direct station that this frame is sent to,* as the frame could be relayed through a wireless bridge or repeater



- Body: It can be up to 2306 bytes and references only two MAC addresses, just like any other Ethernet L2 frame.
- check sequence (FCS) following the L2 frame, this is common but not required.

Frame Types

- all frames are going to have the same type of header.
- The difference is in the body of the frame.
- The body is more specific and indicates what the frame is all about.

Frame Types Table

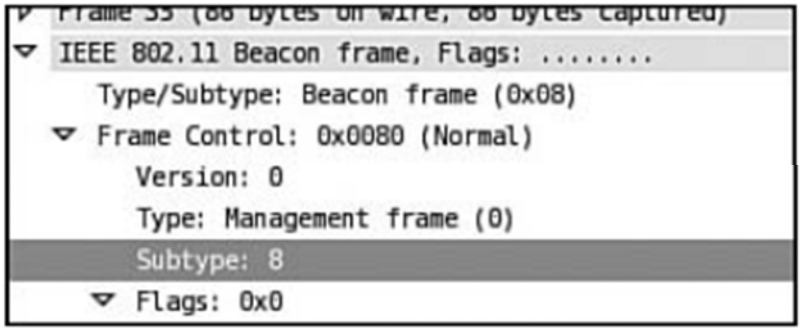
Management	Control	Data
Beacon	Request to Send (RTS)	Simple data
Probe Request	Clear to Send (CTS)	Null function
Probe Response	Acknowledgment	Data+CF-ACK
Association Request	Power-Save-Poll (PS-Poll)	Data+CF-Poll
Association Response	Contention Free End (CF-End)	Data+CF-Ack
Authentication Request	Contention Free End + Acknowl-edgment (CF-End +ACK)	ACK+CF-Poll
Authentication Response	CF-ACK	
Deauthentication	CF-ACK+CF-Poll	
Reassociation request		
Reassociation response		
Announcement traffic indication message (ATIM)		
Each frame type merits its own discussion to follow.		

1. Management Frames

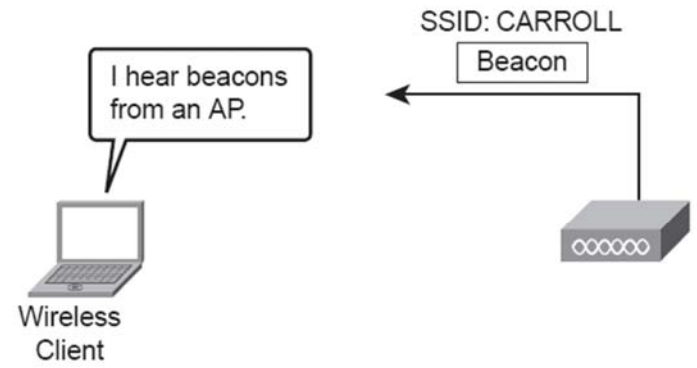
- Are used to manage the connection
- Type field indicates Management, and the subtype tells what kind of management frame it is.
- there are 11 Management frame types.

1.1 Beacons and Probes

- is used to help clients find the network.



- When the client hears the beacon frame, it can learn a great deal of information about the cell.



Sample Network Using Beacon Frames

```
IEEE 802.11 wireless LAN management frame
  Fixed parameters (12 bytes)
    Timestamp: 0x0000000A7341A18A
    Beacon Interval: 0.102400 [Seconds]
    Capability Information: 0x0401
      .... .... .... ...1 = ESS capabilities: Transmitter is an AP
      .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
      .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
      .... .... ...0 .... = Privacy: AP/STA cannot support WEP
      .... .... ..0. .... = Short Preamble: Short preamble not allowed
      .... .... .0.. .... = PBCC: PBCC modulation not allowed
      .... .... 0... .... = Channel Agility: Channel agility not in use
      .... ...0 .... .... = Spectrum Management: dot11SpectrumManagementRequired FALSE
      .... .1.. .... .... = Short Slot Time: Short slot time in use
      .... 0... .... .... = Automatic Power Save Delivery: apsd not implemented
      ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
      .0.. .... .... .... = Delayed Block Ack: delayed block ack not implemented
      0... .... .... .... = Immediate Block Ack: immediate block ack not implemented
  Tagged parameters (52 bytes)
    SSID parameter set: "carroll"
    Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) 18.0 24.0(B) 36.0 54.0
    DS Parameter set: Current Channel: 6
    Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
```

Beacon Frame Details

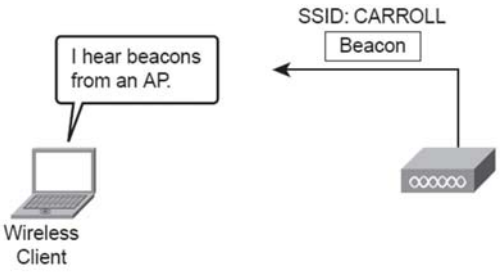
beacon frame includes a

- timestamp that gives a reference time for the cell,
- beacon interval,
- Capability Information, which provides specifics for this cell.

  The Capability Information field includes information regarding power save mode, authentication, and preamble information.
- A beacon frame also includes the SSIDs that the AP supports,
- the rates that are supported, and
- six fields called **Parameter Set** that indicate modulation methods and channel number.

- **Traffic Indication Map (TIM),** which indicates whether the AP is buffering traffic for clients in power-save mode.

When a client sees a beacon frame, it should be able to use that information to determine if it is able to connect to the wireless Cell.

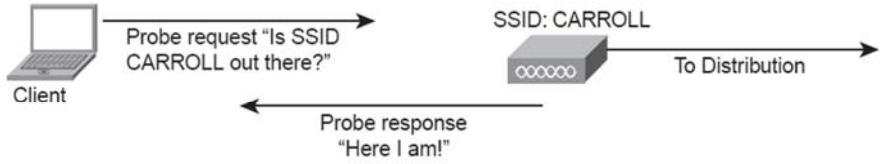


Dr. Ahmed ElShaf

Sample Network Using Beacon Frames

1.2 Prob request, response

- Sometimes, however, you do not want to passively scan a network.
- Perhaps you know exactly what cell you want to connect to.
- In this situation, you can actively scan a network to determine if the cell you are looking for is accessible.
- When a client actively scans a network, it uses probe request and probe response messages.

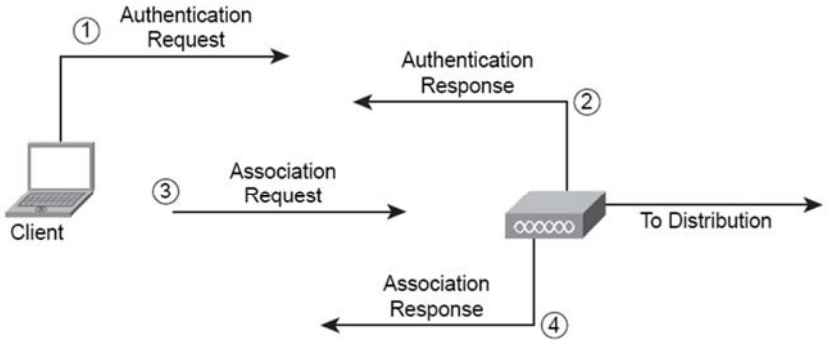


Active Scanning

- the client is looking for a wireless cell with the SSID of "Carroll."
- This client sends a probe request and the AP, upon receiving the probe request, issues a probe response.
- The probe response is similar to the beacon frame, including capability information, authentication information, and so on.
- The difference is that a beacon frame is sent frequently and a probe response is sent only in response to a probe request.

1.3 authentication/ Association frames

- After a client has located an AP and understands the capabilities, it tries to connect using an authentication frame
- This frame has information about
  - the algorithm used to authenticate,
  - a number for the authentication transaction, and
  - information on whether authentication has succeeded or failed.
- One thing to note is that authentication can be *Open, meaning that no authentication algorithm* such as WEP is being used.
- The only reason an authentication message is used is to indicate that the client has the capability to connect.



Authentications and Association

1. the client is sending an authentication request,
2. AP is sending an authentication response.
3. Upon authentication, the client sends an association request,
4. AP responds with an association response.

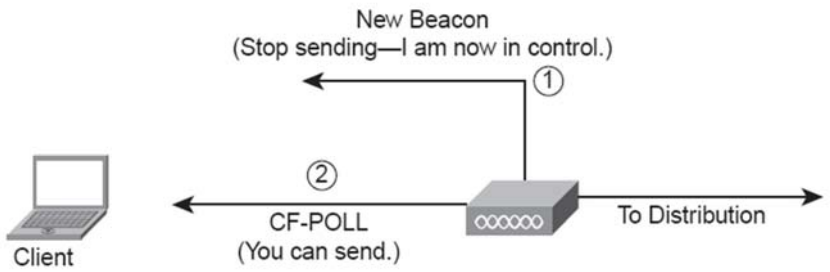
1.4 de-authentication/ disassociation / re-association frames

- When a client is connected to a wireless cell, either the client or the AP can leave the connection by sending a de-authentication message
- The de-authentication message has information in the body as to why it is leaving
- a client can send a disassociation message, which disassociates the client from the cell but keeps the client authenticated.
- The next time a client comes back to the wireless cell, it can simply send a re-association message,

2. Control Frames

- The most common control frames is the ACK, which helps the connection by acknowledging receipt of frames.
- Other control frames include the request to send (RTS) and clear to send (CTS),
- The control frames that are used in PCF (Point of Coordination function) mode are as follows:
  - Contention Free End (CF+End)
  - Contention Free End Ack (CF +end+ack)
  - CF-Ack
  - CF-Poll

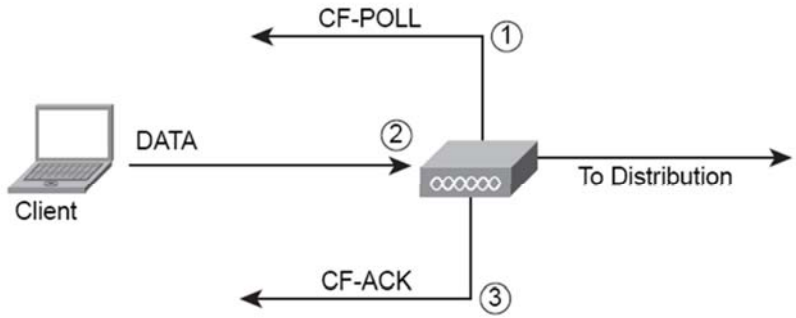
- When an AP takes control of a network and shifts from DCF mode (every station for itself) to PCF mode (the AP is responsible for everyone sending), the AP lets all stations know that they should stop sending by issuing a beacon frame with a duration of 32768.



CF-Poll in PCF Mode

- When this happens and everyone stops sending, there is no longer a contention for the medium, because the AP is managing it.
- This is called a ***contention free window*** *(CFW).*

- Client has data to be delivered to AP, AP sens CF-POLL to client.
- It allows the client to send data (CF-Poll) and acknowledges receipt of the client data (CF-ACK).



Power Save Mode and Frame Types

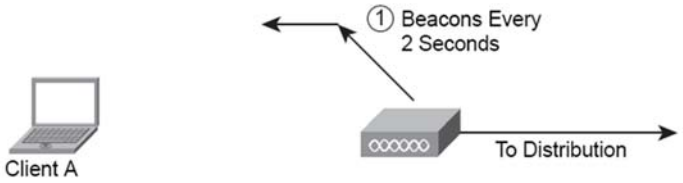
- Another mode of operation mostly seen on laptops is called power save mode
- Uses power save (PS-Poll).
- power save, a client notifies an AP that it is falling asleep by using a null function frame.
- The client wakes up after a certain period of time, during which the AP buffers any traffic for it.
- When the client wakes up and sees a beacon frame with the **Traffic Indication Map (TIM),** listing that it has frames buffered, the client sends a PS-Poll requesting the data.

Frame Speeds

- The AP advertises mandatory speeds at which a client must be able to operate.
- You can use other speeds, but they are not mandatory.
- For example, 24 Mbps might be mandatory, but an AP might also be capable of 54 Mbps.
- A client *must support 24 Mbps but is allowed to use the best rate* possible, in this example 54 Mbps.
- When data is sent at one rate, the ACK is always sent at 1 data rate lower.

A Wireless Connection, the whole story

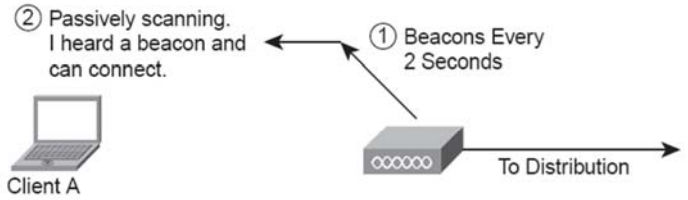
1. The AP sends beacons every 2 seconds,



AP Beacons

2. Client A is passively scanning and hears the beacon.

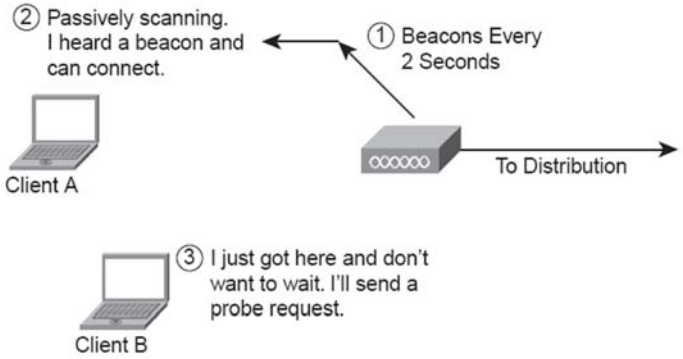
   This enables the client to determine whether it can connect



Passive Scanning

3. A new client (Client B) arrives.

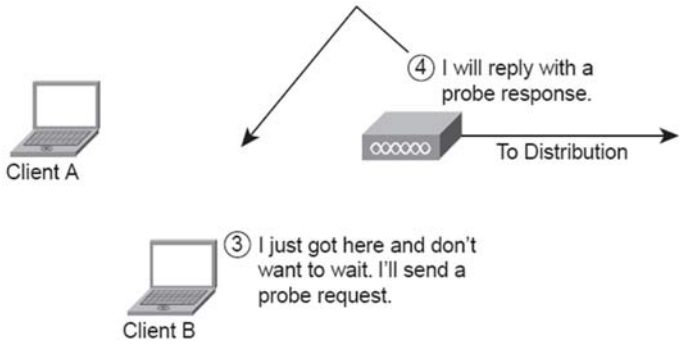
   Client B is already configured to look for the AP, so instead of passive scanning, it sends a probe request for the specific AP



Active Scanning Probe Request

4. The AP sends a probe response, which is similar to a beacon.

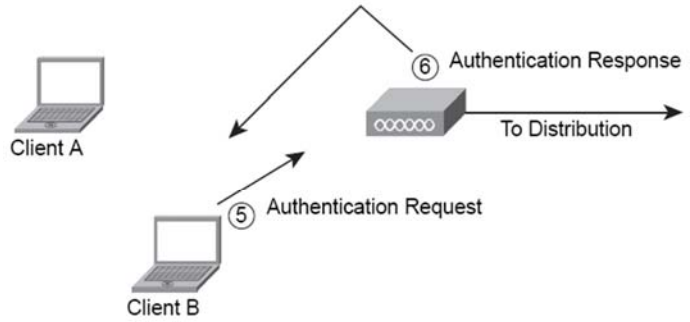
   This lets Client B determine if it can connect.



Probe Response

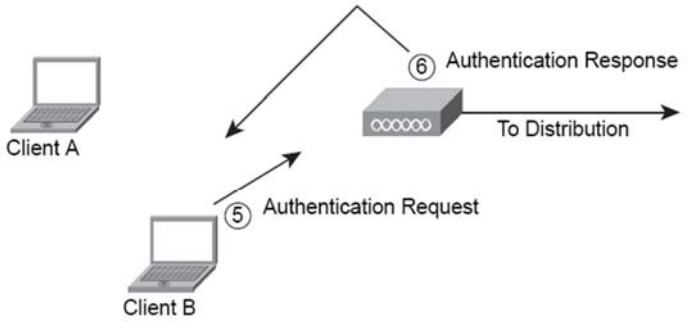
5. From this point on, the process would be the same for Client A and Client B.

Client B sends an authentication request.



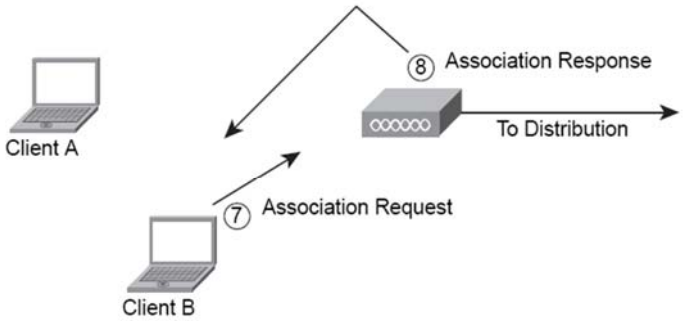
Association Request and Response

6. the AP returns an authentication response to the client.



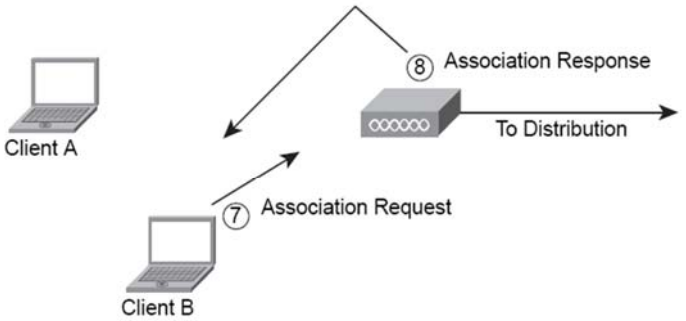
Association Request and Response

7. The client then sends an association request



Association Request and Response

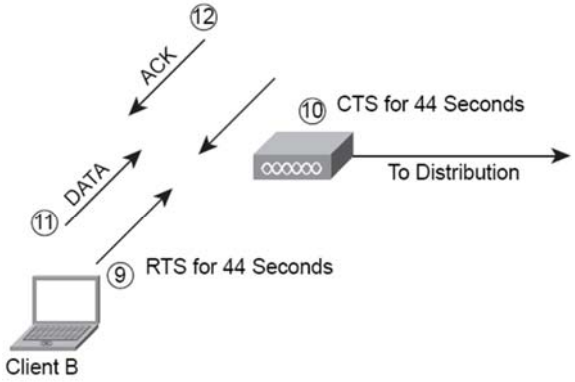
8. Now the AP sends an association response



Association Request and Response

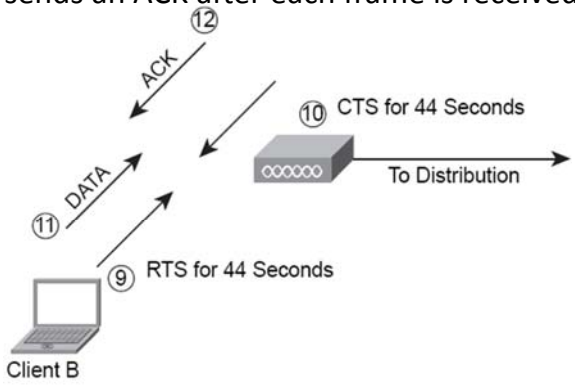
9. When the client wants to send, it uses an RTS, assuming this is a mixed b/g cell.

   The RTS includes the duration



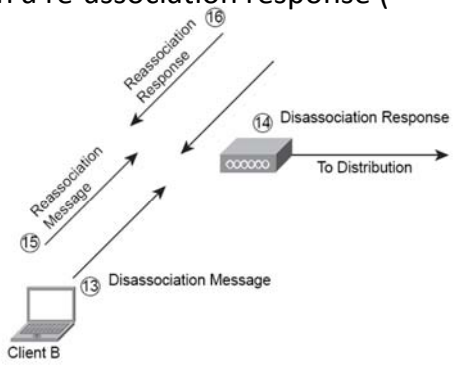
RTS/CTS

10. the AP returns a CTS
11. The client sends the data
12. The AP sends an ACK after each frame is received



RTS/CTS

13. the client sends a disassociation message.
14. The AP replies with a disassociation response
15. The client returns and sends a re-association message
16. The AP responds with a re-association response (



Reassociation

Thanks,

See you next Week, isA