Wireless Technology Applications

Wireless Local Area Network Technology Part II

Melvyn U Myint Oo
T16620
68790688
melvyn_oo@sp.edu.sg

At the end of this lecture, you should be able to:

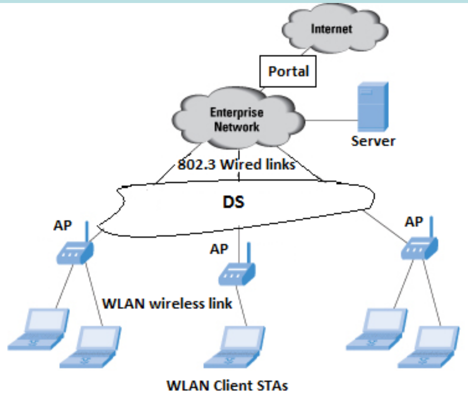
Explain WLAN technology

1. MAC Functional Operation
2. Frame Format
3. Logical Service
4. Power Management
5. IEEE 802.11 Securities
6. Examples of WLAN Applications
7. Advantages of WLANs

But first…

Wireless LAN MAC

- **M**edium **A**ccess **C**ontrol
- MAC layer enables different STAs to communicate with the AP



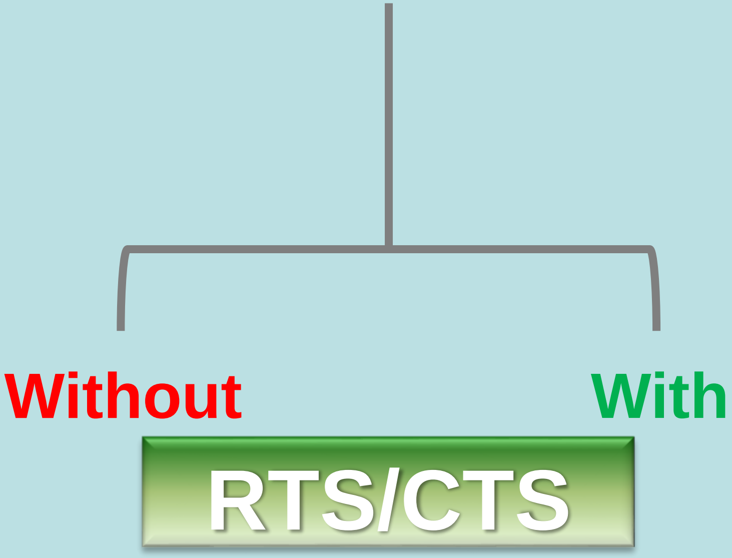
What we want to avoid…

But how?

Official (Open), Non-sensitive

Distributed Coordination Function (DCF)

- **C**arrier **S**ensing **M**ultiple **A**ccess / **C**ollision **A**voidance (**CSMA/CA**)
  - “Listen before send”



Without

With

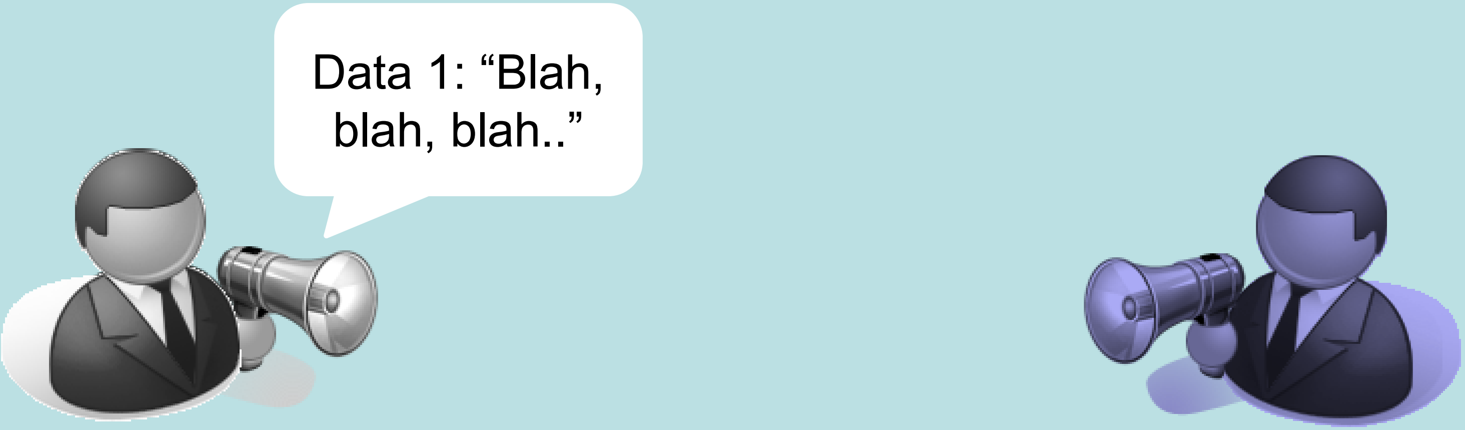
RTS/CTS

CSMA/CA

- Example 3.9
- IEEE802.11 specifies the Data Link layer by using CSMA/CA instead of CSMA/CD in wired networks. Why is there a need to change from collision detection to collision avoidance?
- Due to the wireless medium, it is not possible to allow multiple STAs to transmit together without interference over the same frequency at the same time and without the use of orthogonal codes.
- Also, antennas are not able to transmit and receive over the same frequency at the same time.
- As a result, collision detection is not possible because it requires sending packets and listening packets at the same time.
- Since collision detection is impossible in wireless medium, mechanism has to be in placed to avoid collision.

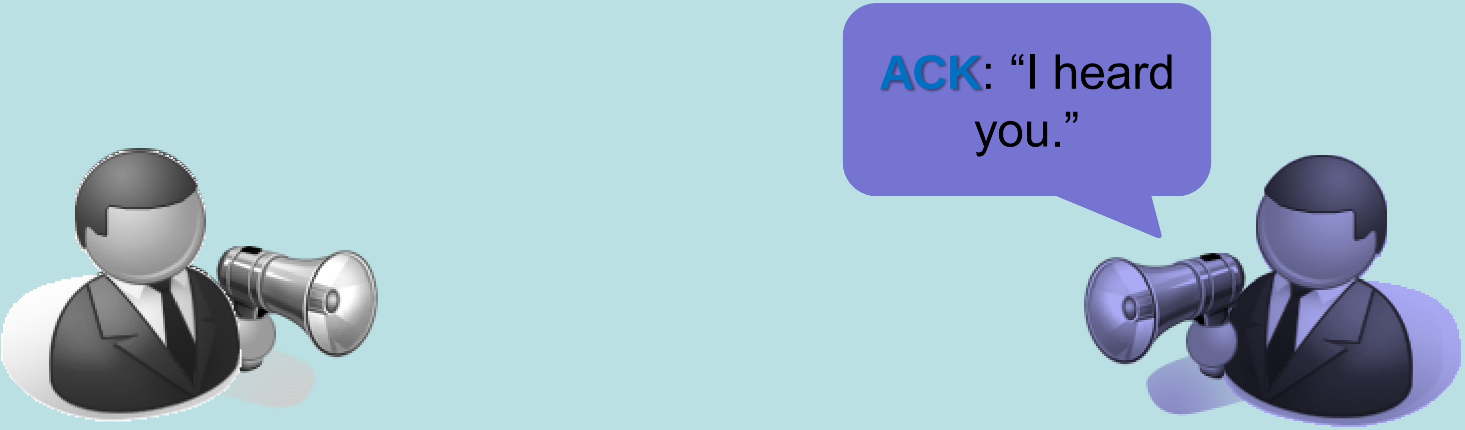
CSMA/CA

- **Mechanisms used**
  - Acknowledgement (ACK) frame



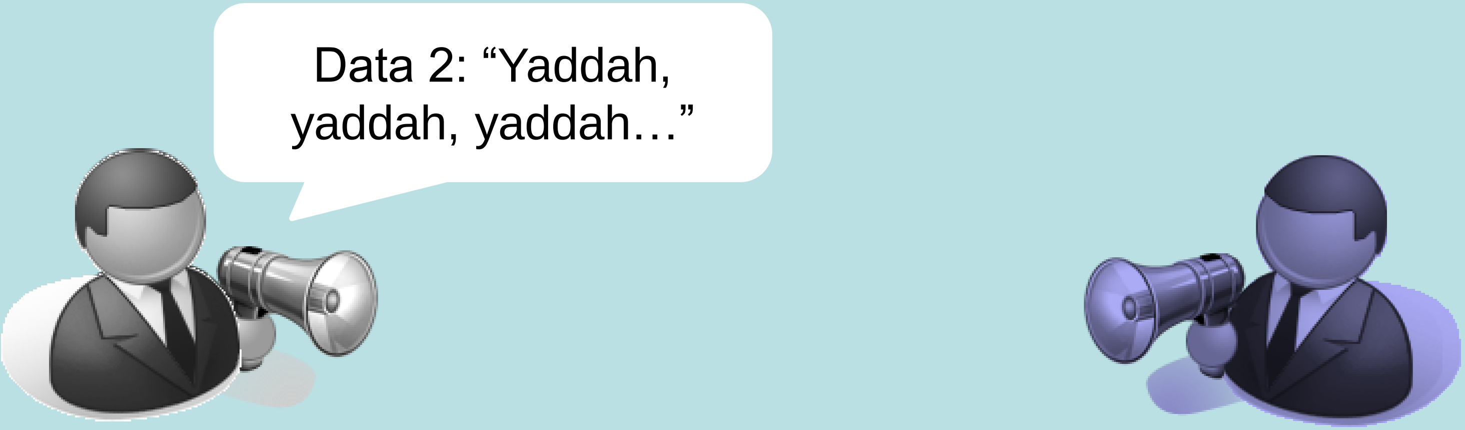
CSMA/CA

- **Mechanisms used**
  - Acknowledgement (ACK) frame



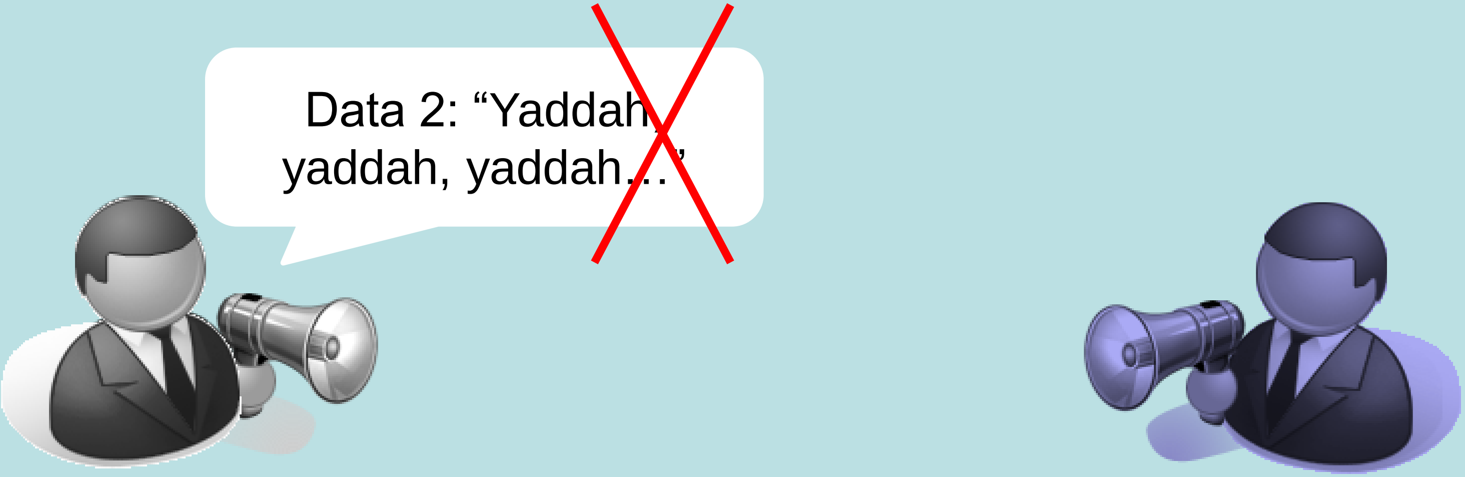
CSMA/CA

- **Mechanisms used**
  - Acknowledgement (ACK) frame



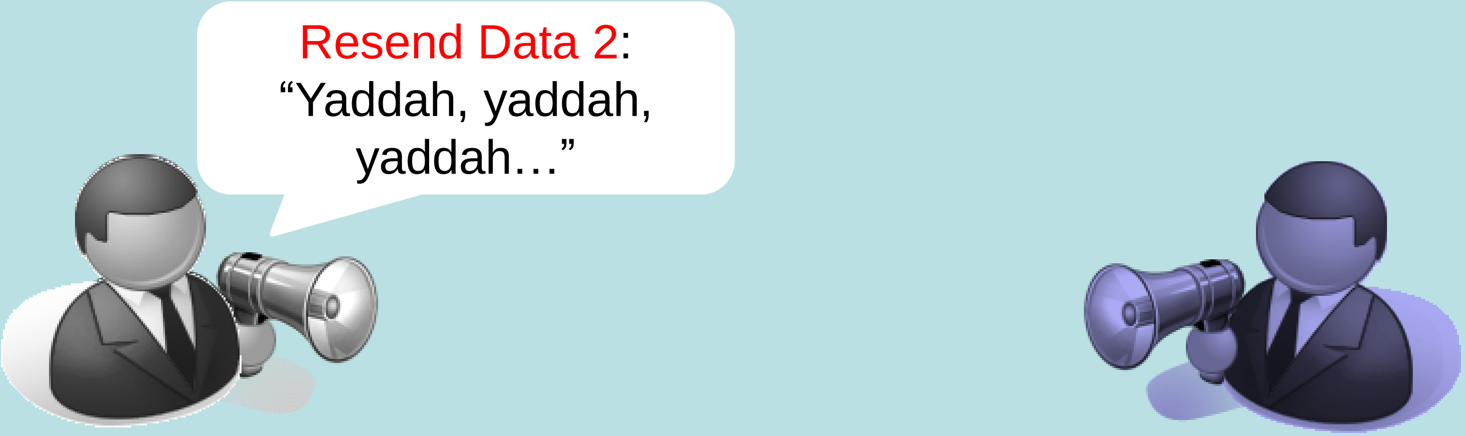
CSMA/CA

- **Mechanisms used**
  - Acknowledgement (ACK) frame



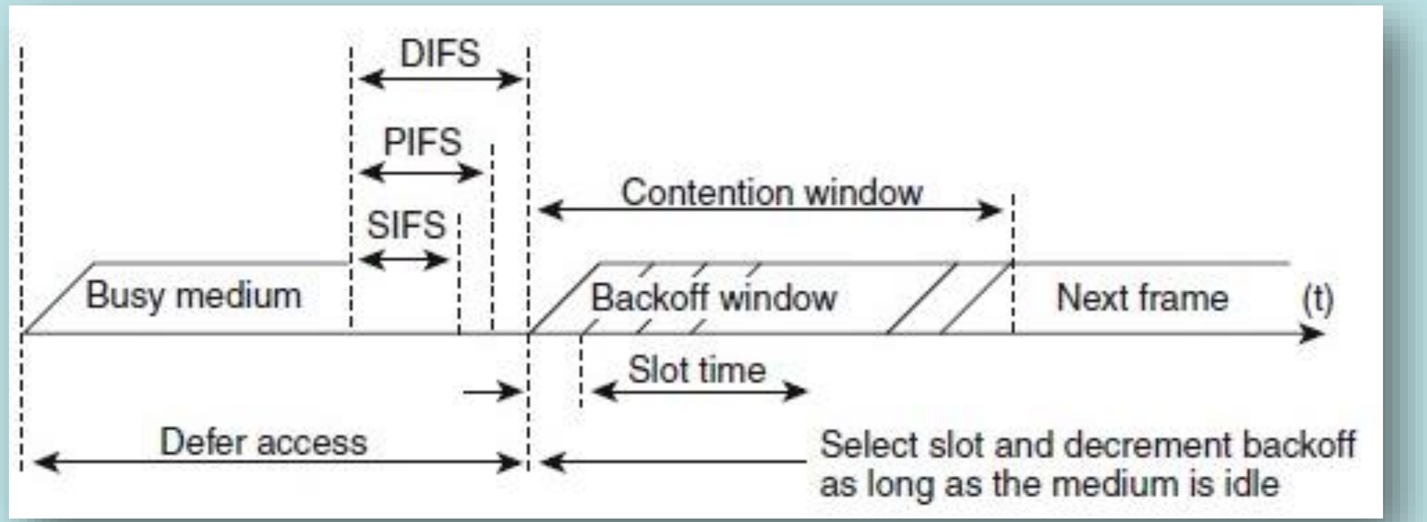
CSMA/CA

- **Mechanisms used**
  - Acknowledgement (ACK) frame



CSMA/CA

- **Mechanisms used**
  - Acknowledgement (ACK) frame
  - Short Inter-Frame Space (SIFS) vs DCF Inter-Frame Space (DIFS)
  - Random backoff counter

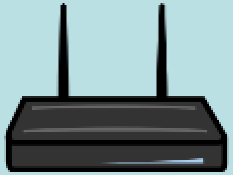


CSMA/CA

- Example 3.10
- What is the purpose of the random backoff interval in CSMA?
- The random backoff interval attempts to prevent two or more STAs that are waiting for the wireless medium to be available from transmitting together once it is idle.

CSMA/CA without RTS/CTS

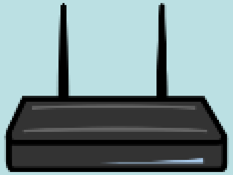
1. Senses that wireless medium is free



Hmm… No one else is sending

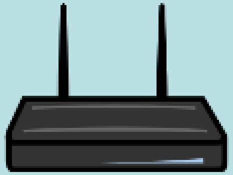
CSMA/CA without RTS/CTS

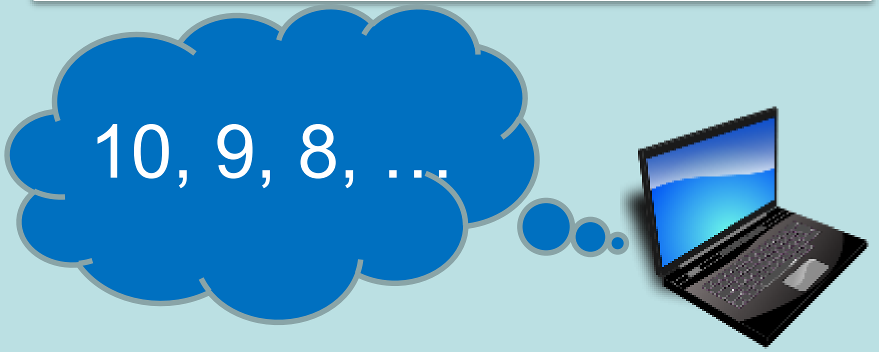
1. Senses that wireless medium is free
2. Waits for DIFS



CSMA/CA without RTS/CTS

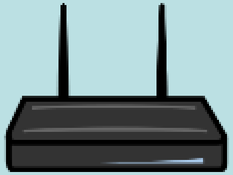
1. Senses that wireless medium is free
2. Waits for DIFS
3. Starts decrease Random Backoff counter, waiting…





CSMA/CA without RTS/CTS

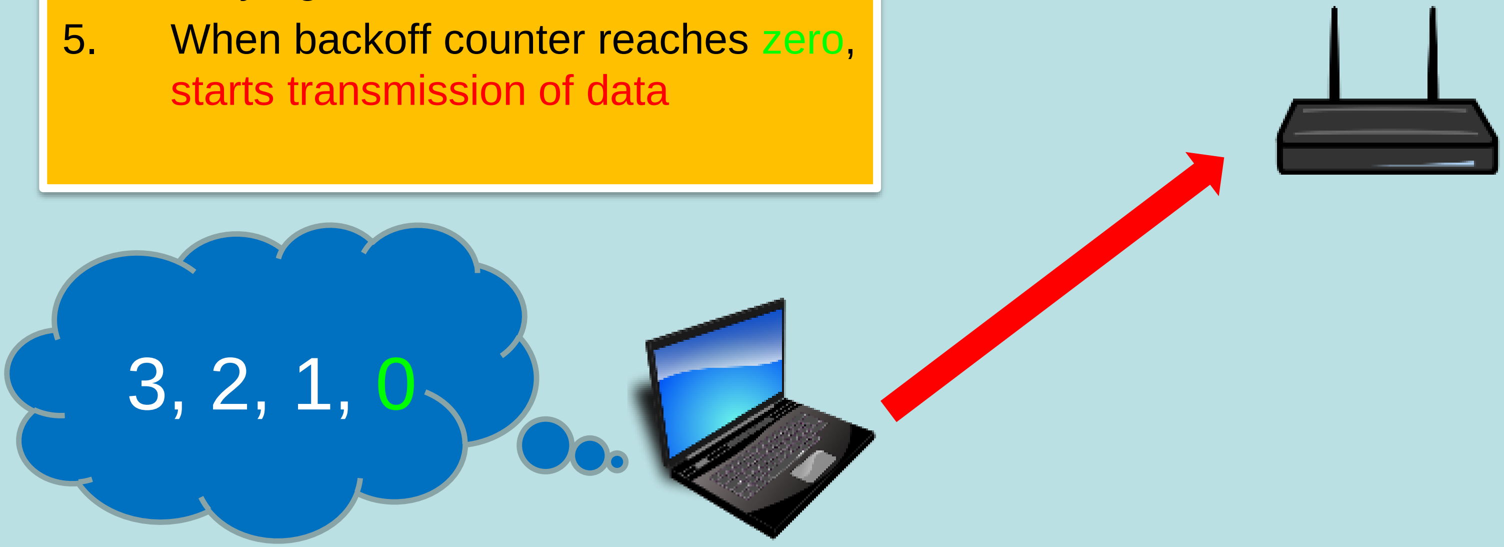
1. Senses that wireless medium is free
2. Waits for DIFS
3. Starts decrease Random Backoff counter, waiting…
4. Listens if wireless medium becomes busy again



Official (Open), Non-sensitive

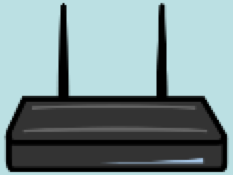
CSMA/CA without RTS/CTS

1. Senses that wireless medium is free
2. Waits for DIFS
3. Starts decrease Random Backoff counter, waiting…
4. Listens if wireless medium becomes busy again
5. When backoff counter reaches zero, starts transmission of data



CSMA/CA without RTS/CTS

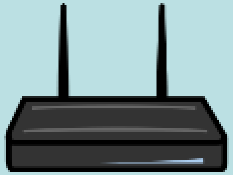
1. Senses that wireless medium is free
2. Waits for DIFS
3. Starts decrease Random Backoff counter, waiting…
4. Listens if wireless medium becomes busy again
5. When backoff counter reaches zero, starts transmission of data
6. Completes transmission



CSMA/CA without RTS/CTS

1. Senses that wireless medium is free
2. Waits for DIFS
3. Starts decrease Random Backoff counter, waiting…
4. Listens if wireless medium becomes busy again
5. When backoff counter reaches zero, starts transmission of data
6. Completes transmission

1. Receives data transmission



CSMA/CA without RTS/CTS

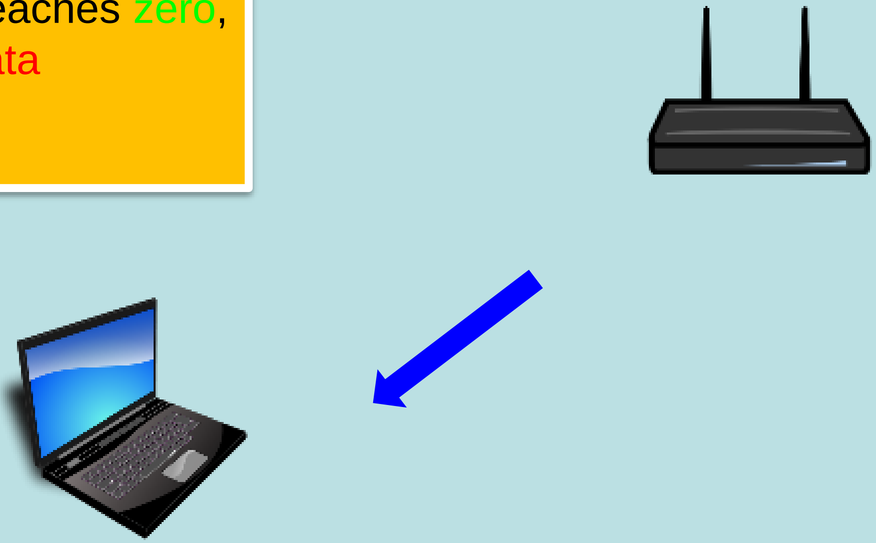
1. Senses that wireless medium is free
2. Waits for DIFS
3. Starts decrease Random Backoff counter, waiting…
4. Listens if wireless medium becomes busy again
5. When backoff counter reaches zero, starts transmission of data
6. Completes transmission

1. Receives data transmission
2. Waits for SIFS

CSMA/CA without RTS/CTS

1. Senses that wireless medium is free
2. Waits for DIFS
3. Starts decrease Random Backoff counter, waiting…
4. Listens if wireless medium becomes busy again
5. When backoff counter reaches zero, starts transmission of data
6. Completes transmission

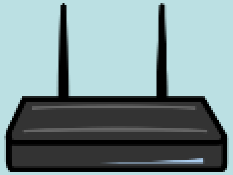
1. Receives data transmission
2. Waits for SIFS
3. Transmits Acknowledgement frame



CSMA/CA without RTS/CTS

1. Senses that wireless medium is free
2. Waits for DIFS
3. Starts decrease Random Backoff counter, waiting…
4. Listens if wireless medium becomes busy again
5. When backoff counter reaches zero, starts transmission of data
6. Completes transmission
7. Selects new backoff value

1. Receives data transmission
2. Waits for SIFS
3. Transmits Acknowledgement frame

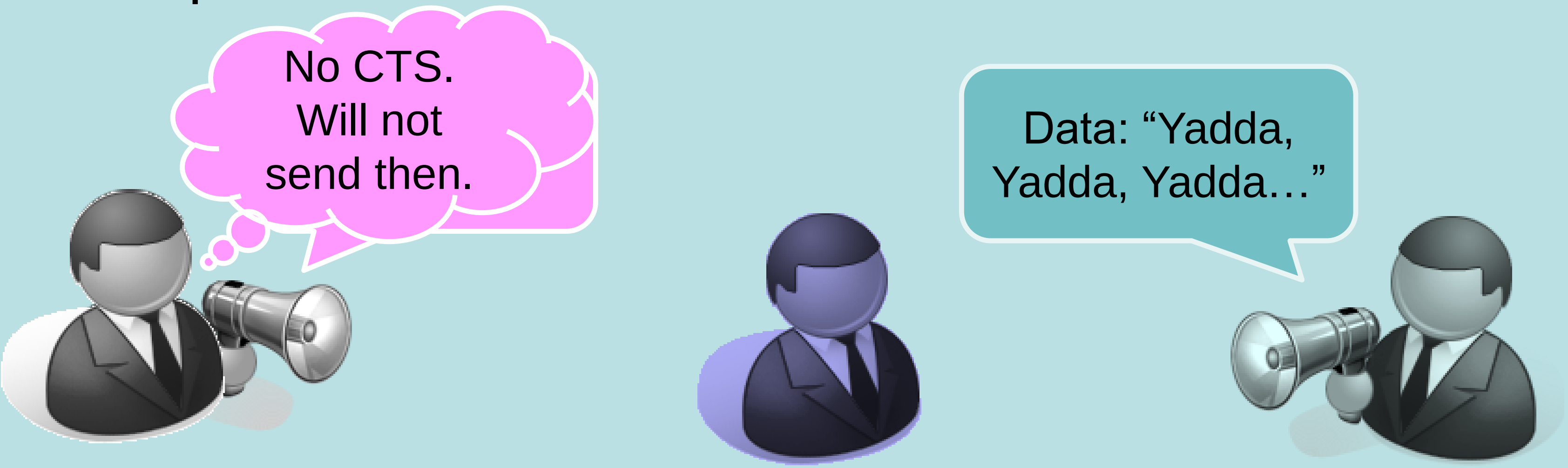


Backoff = 15

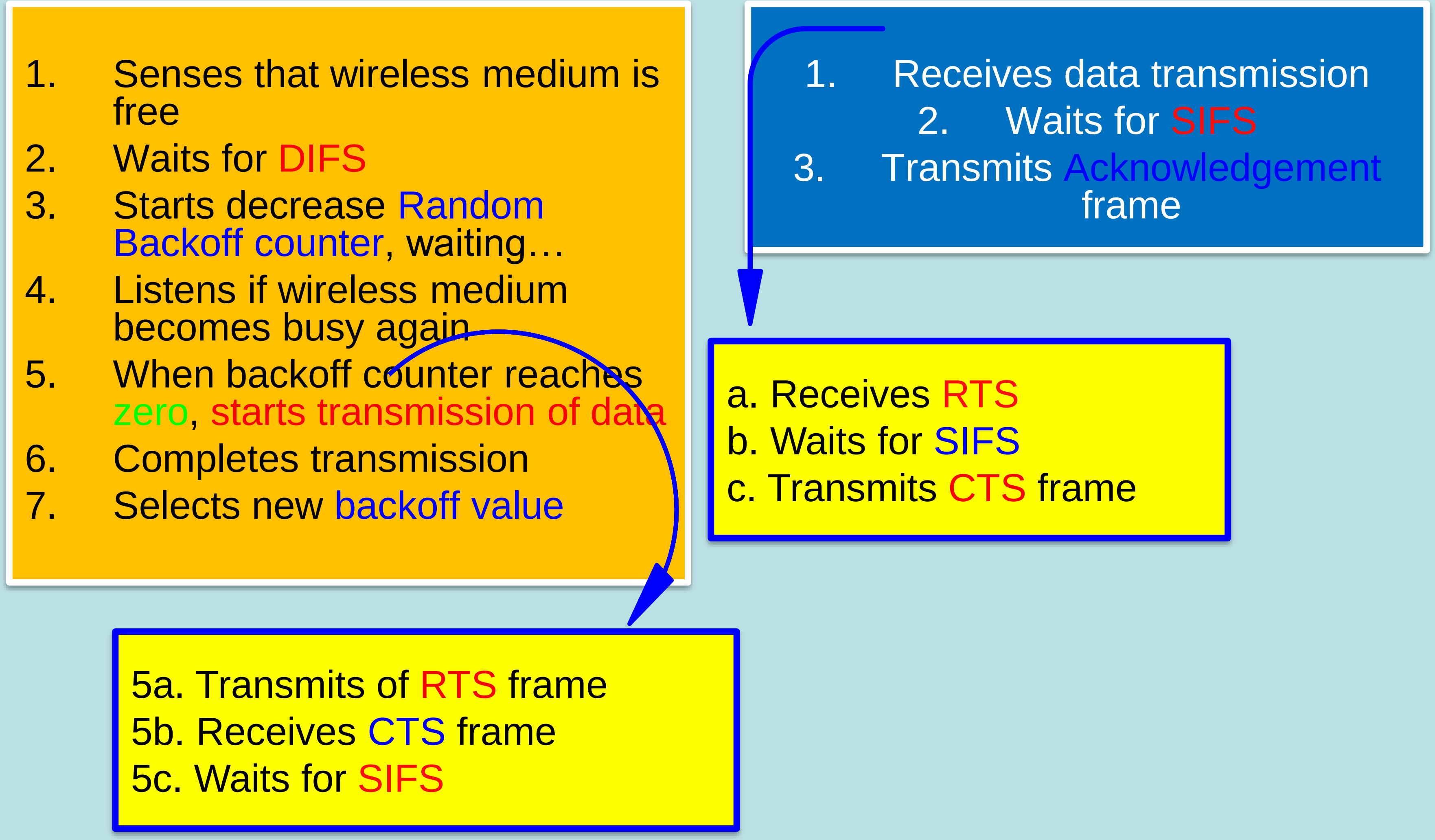
CSMA/CA with RTS/CTS

- RTS – Request To Send
- CTS – Clear To Send

Example 2



CSMA/CA with RTS/CTS



1. Senses that wireless medium is free
2. Waits for DIFS
3. Starts decrease Random Backoff counter, waiting…
4. Listens if wireless medium becomes busy again
5. When backoff counter reaches zero, starts transmission of data
6. Completes transmission
7. Selects new backoff value

5a. Transmits of RTS frame
5b. Receives CTS frame
5c. Waits for SIFS

a. Receives RTS
b. Waits for SIFS
c. Transmits CTS frame

1. Receives data transmission
2. Waits for SIFS
3. Transmits Acknowledgement frame

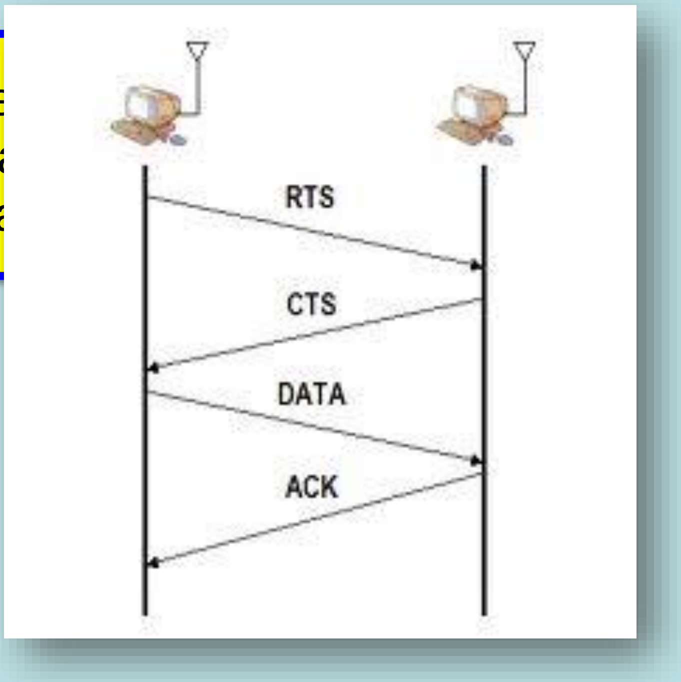
CSMA/CA with RTS/CTS

1. Senses that wireless medium is free
2. Waits for DIFS
3. Starts decrease Random Backoff counter, waiting…
4. Listens if wireless medium becomes busy again
5. When backoff counter reaches zero, starts transmission of data
6. Completes transmission
7. Selects new backoff value

5a. Transmits of RTS frame
5b. Receives CTS frame
5c. Waits for SIFS

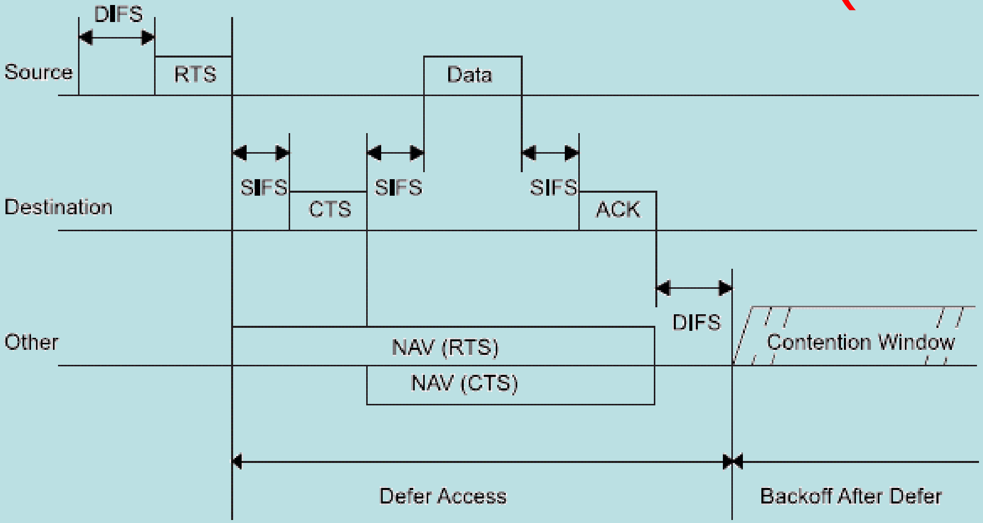
1. Receives data transmission
2. Waits for SIFS
3. Transmits Acknowledgement frame

a. Re
b. Wa
c. Tra



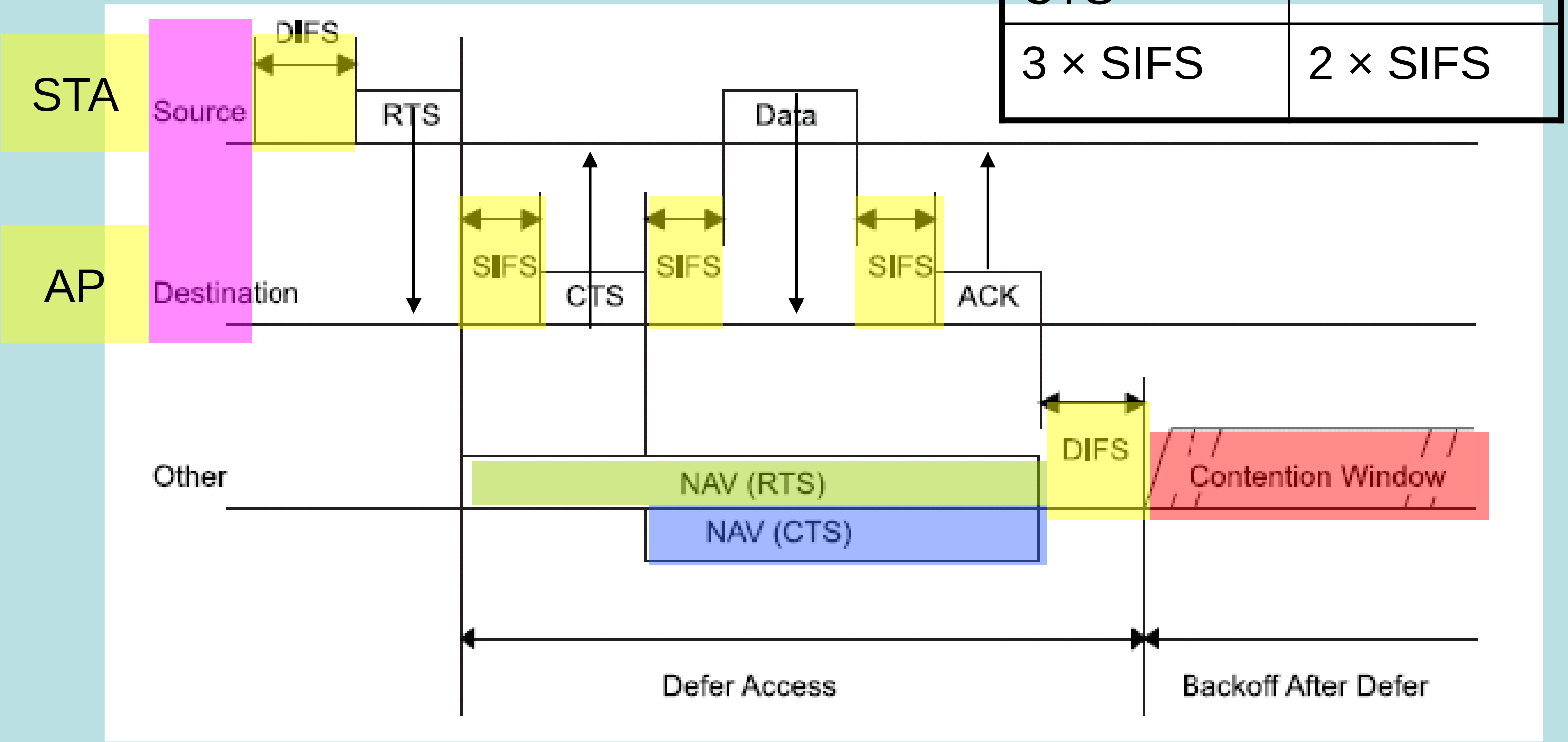
More about RTS/CTS

- RTS and CTS frames contains in its Duration/ID field the amount of time reserved for transmitting the data frame and returning ACK frame.
- Known as Network Allocation Vector (NAV)



NAV Setting

RTS	CTS
Data	Data
ACK	ACK
CTS	
3 × SIFS	2 × SIFS



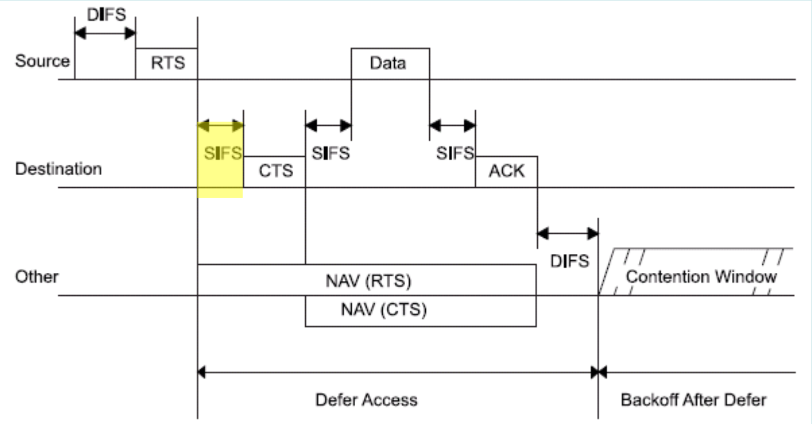
More about RTS/CTS

- CSMA/CA Without RTS/CTS
  – Known as Physical Carrier Sensing
- CSMA/CA With RTS/CTS
  – Known as Virtual Carrier Sensing

In general, DCF uses CSMA/CA which means that anyone (either STA or AP) can send whenever the wireless medium is sensed to be free

InterFrame Space (IFS)

- Example 3.11
- In Figure 3.10, explain why the IFS (InterFrame Space) between RTS and CTS is SIFS (Short IFS)?
- This will ensure that the receiver STA is able to transmit CTS before other STAs have the opportunity to transmit other types of packets since SIFS is the shortest.



Official (Open), Non-sensitive

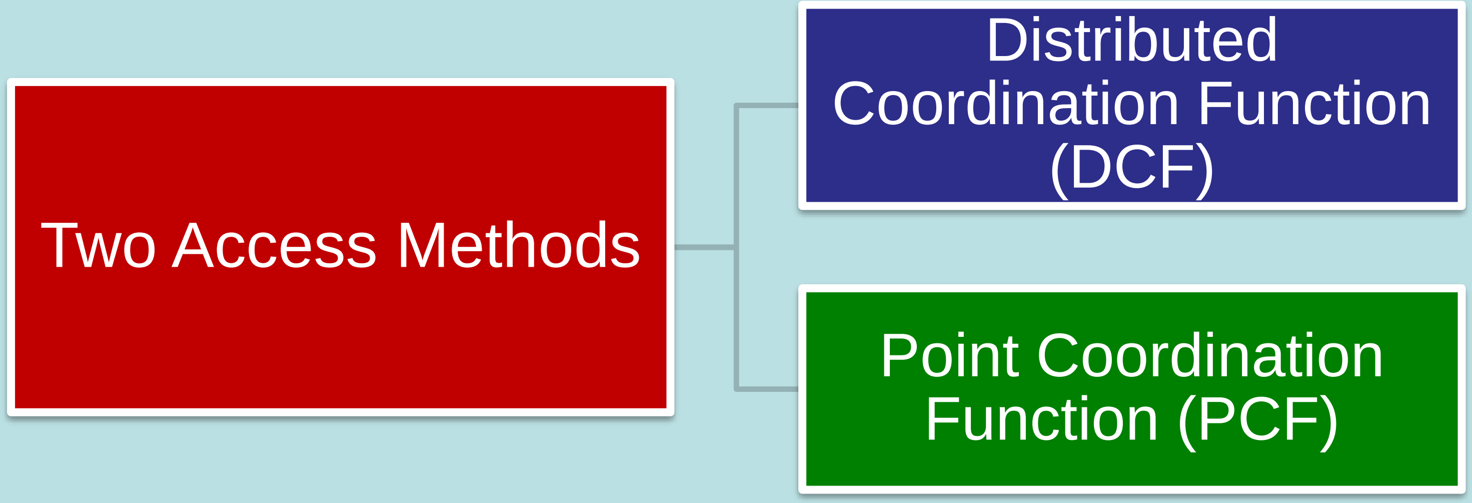
Advantages of Virtual sense over Physical sense mechanisms

- Perform fast inference and transmission path check
- If collision occurs in initial transmission, CTS will not be transmitted by AP. Then, STA can retransmit RTS if channel is still idle instead of waiting for the long data frame to be transmitted completely.

- Work across multiple ESSs and IBSSs
- STAs in multiple ESSs and IBSSs that transmit on the same frequency can receive NAV

- Virtual sense cannot be used in multicast and broadcast since there are more than one receiving STA

In IEEE 802.11…

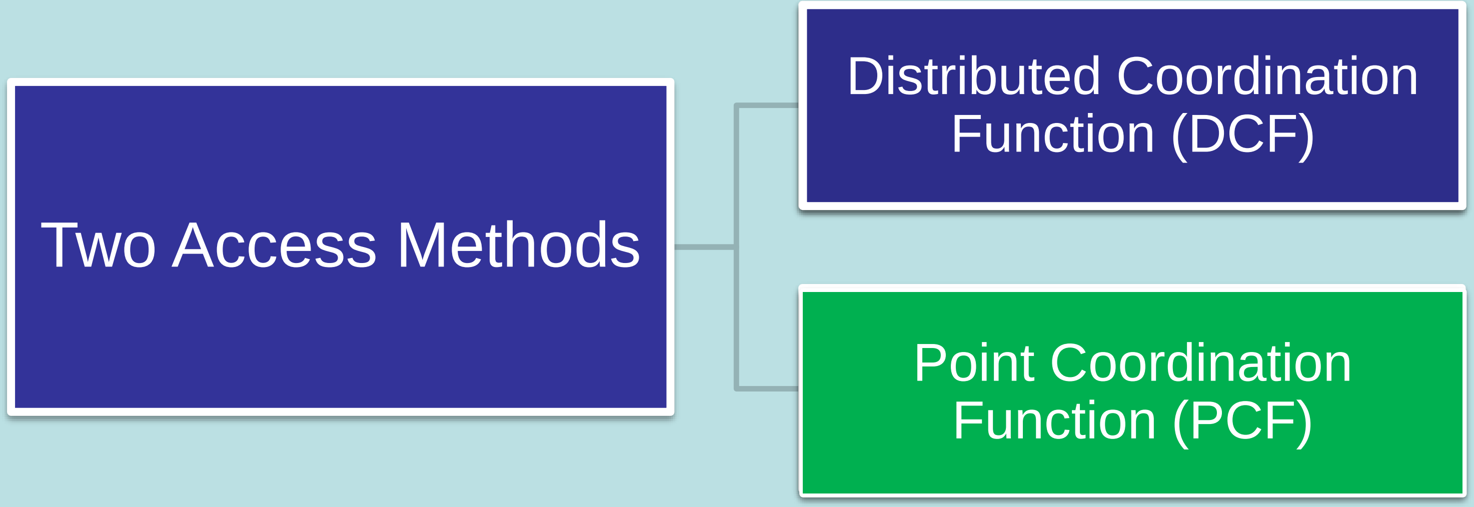


Two Access Methods

Distributed Coordination Function (DCF)

Point Coordination Function (PCF)

Main Differences


Two Access Methods
Distributed Coordination Function (DCF)
Point Coordination Function (PCF)

Main Differences

Distributed Coordination Function (DCF)

Point Coordination Function (PCF)

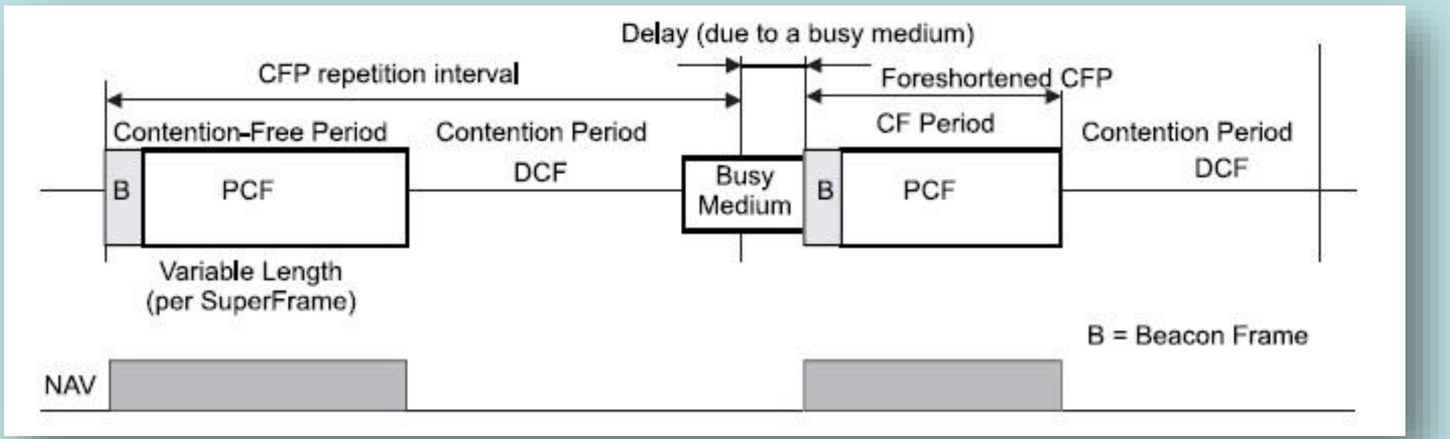
Main Differences

- No central controller
- STAs “try their luck” and resolve collision when it occurs
- Contention (CSMA/CA)

- AP is central controller
- Polling done to prevent collision
- Contention Free

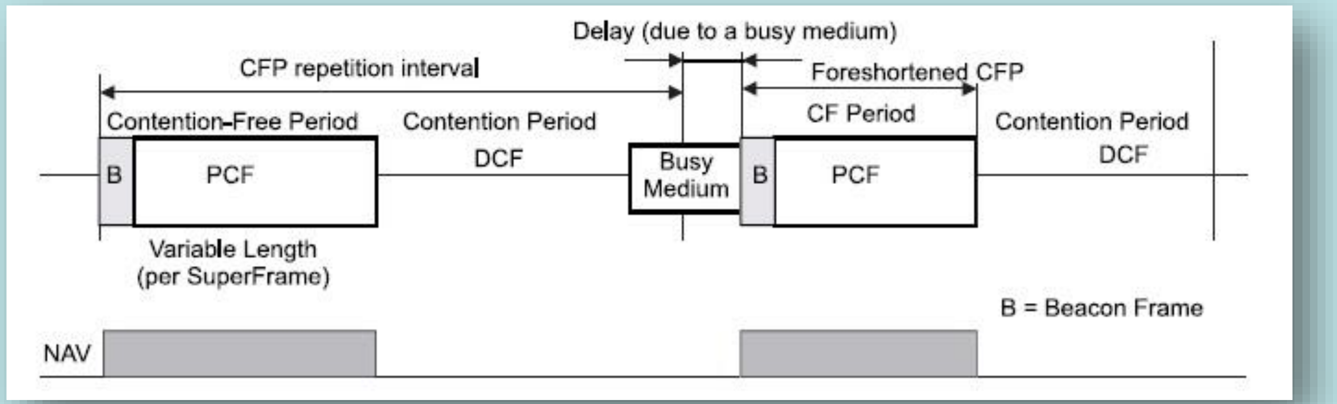
Singapore Polytechnic

Main Differences



Point Coordination Function (PCF)

- Point Coordination Function (PCF) uses polling mechanism
  - AP acts as a polling master (must support PC feature)
  - STA must support (CF-Pollable feature)
- PCF uses Contention-Free Period (CFP) and DCF uses Contention Period (CP)

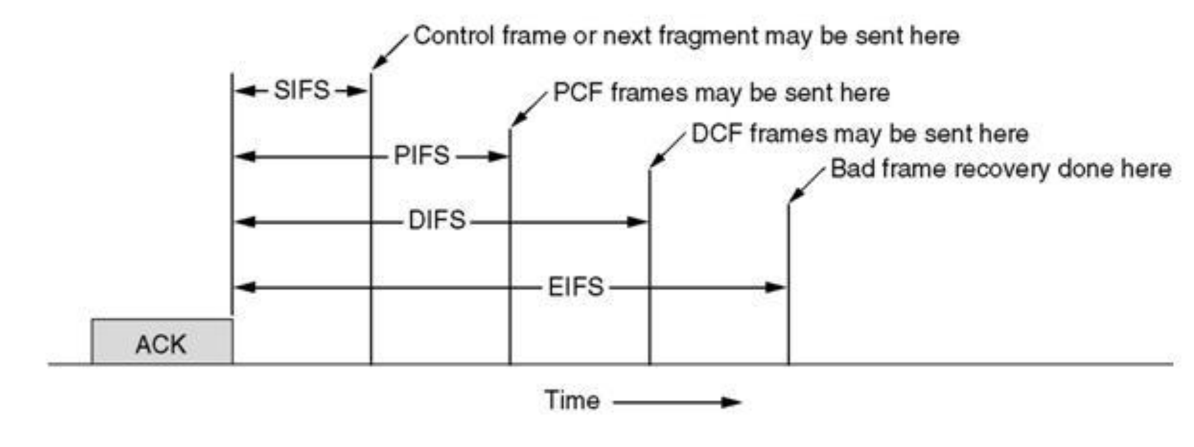


InterFrame Space (IFS)

- Example 3.12
- How does STAs operating in PCF (Point Coordination Function) has a higher priority in gaining access to the wireless medium over STAs operating in DCF (Distribution Coordination Function)?
- PCF uses PIFS (Point Coordination Function IFS) which has shorter interval compared to DIFS (Distribution Coordination Function IFS) used in DCF.

InterFrame Space (IFS)

- SIFS (Short IFS) – ACK, CTS, second or subsequent fragments, STA responding to polling, PC during CFP
- PIFS (PCF IFS) – STAs during PCF (Point Coordination Function)
- DIFS (DCF IFS) – STAs during DCF (Distributed Coordination Function)
- EIFS (Extended IFS) – during DCF when a MAC frame is received incorrectly but with a valid FCS value


Control frame or next fragment may be sent here
SIFS
PCF frames may be sent here
DCF frames may be sent here
Bad frame recovery done here
PIFS
DIFS
EIFS
ACK
Time

Random Backoff Time

- Backoff is randomised to prevent 2 STAs from transmitting at the same time
- Time is divided into slots
- STAs wanting to transmit choose a random number from 0 to 31

I'll choose 2
I'll choose 27

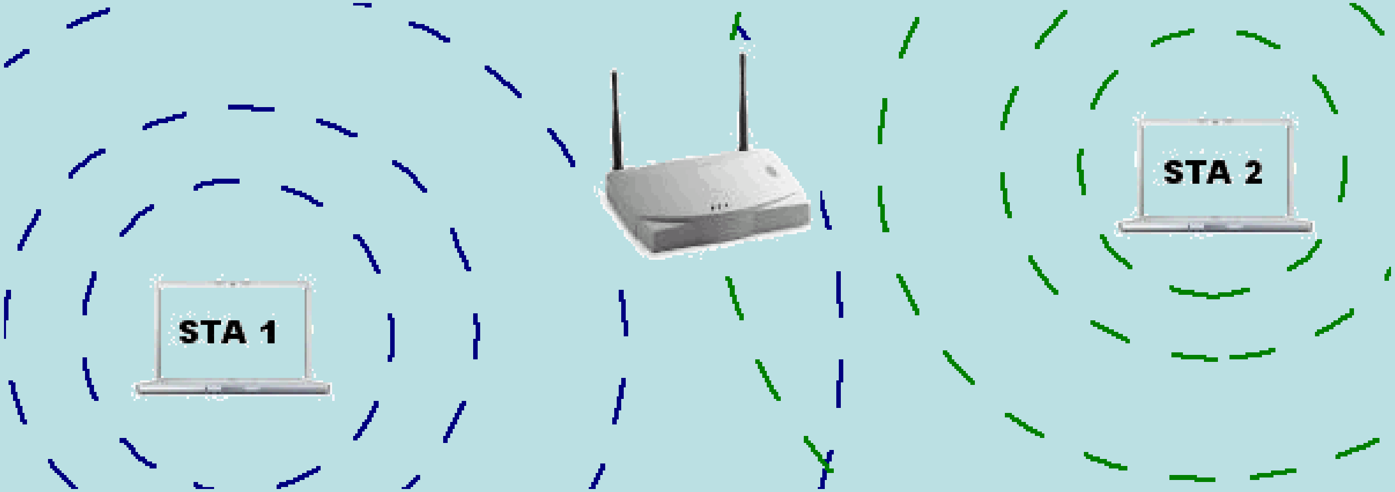
Random Backoff Time

- Backoff is randomised to prevent 2 STAs from transmitting at the same time
- Time is divided into slots
- STAs wanting to transmit choose a random number from 0 to 31
- If transmission fails, STAs will now choose a random number from 0 to 63
- Then, 127, 255, and so on… always 1 less than 2^n

I'll now choose 58
I'll now choose 14

Hidden Node Problem

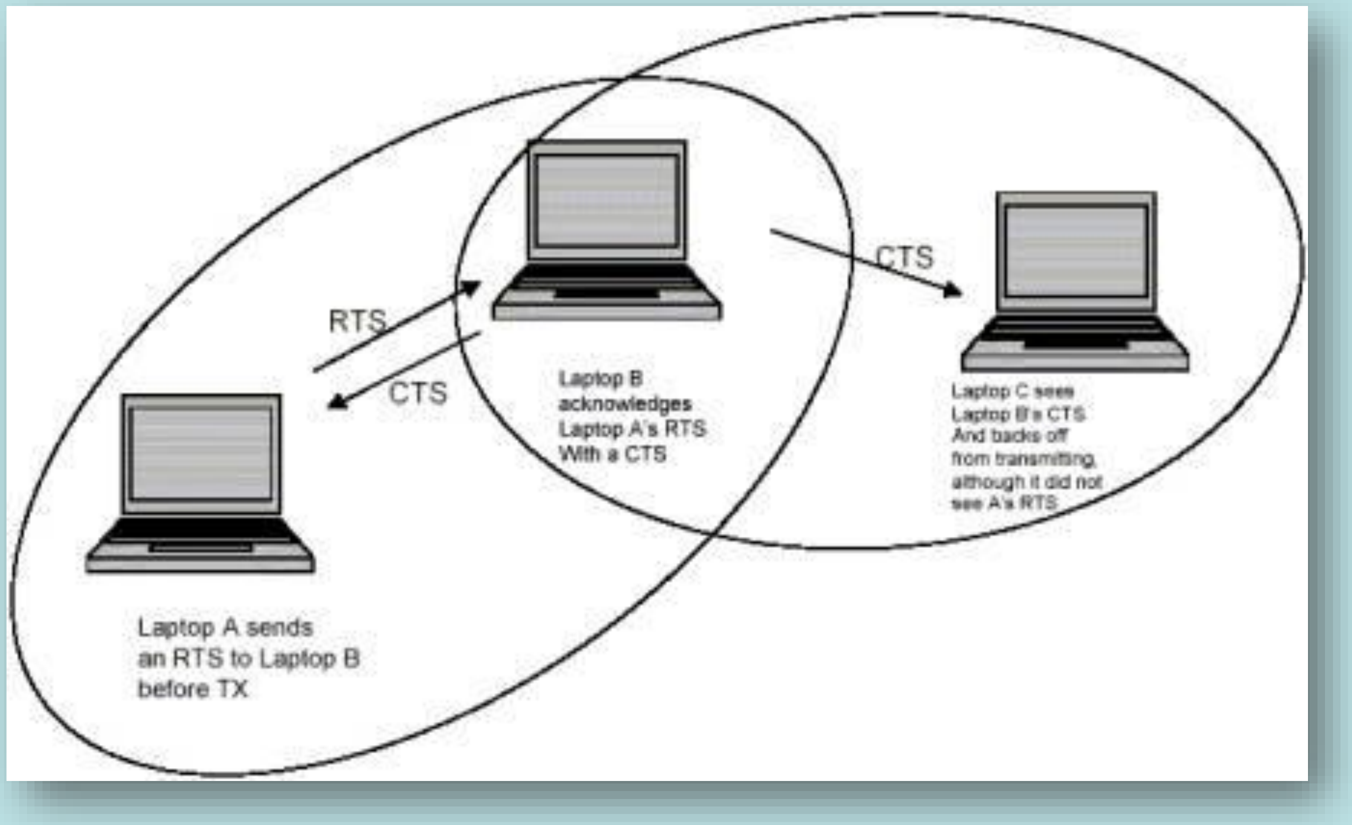
- It is possible that all STAs can communicate with an AP, but the STAs cannot communicate with each other
- One STA can communicate with the AP without knowing that another STA is already communicating with the AP



Singapore Polytechnic

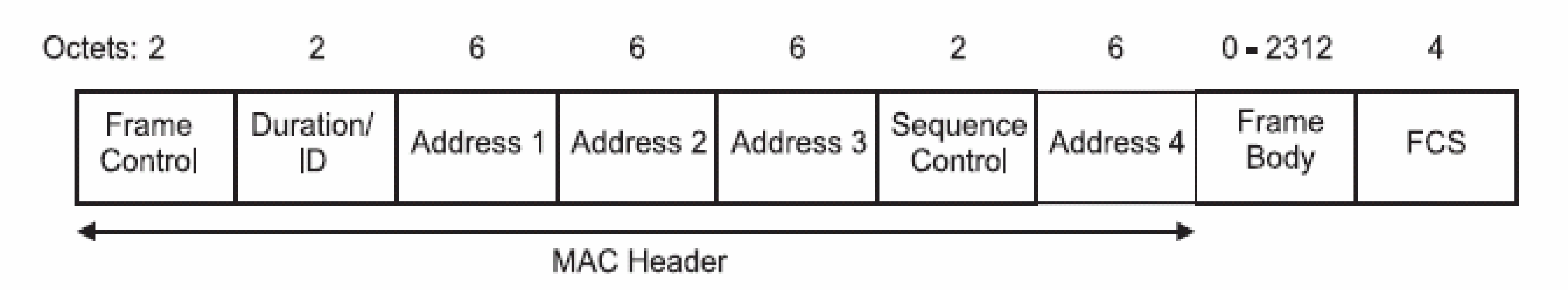
Hidden Node Problem

- Can be solved using RTS/CTS


RTS
CTS
CTS
Laptop B acknowledges Laptop A's RTS With a CTS
Laptop C sees Laptop B's CTS And backs off from transmitting, although it did not see A's RTS
Laptop A sends an RTS to Laptop B before TX

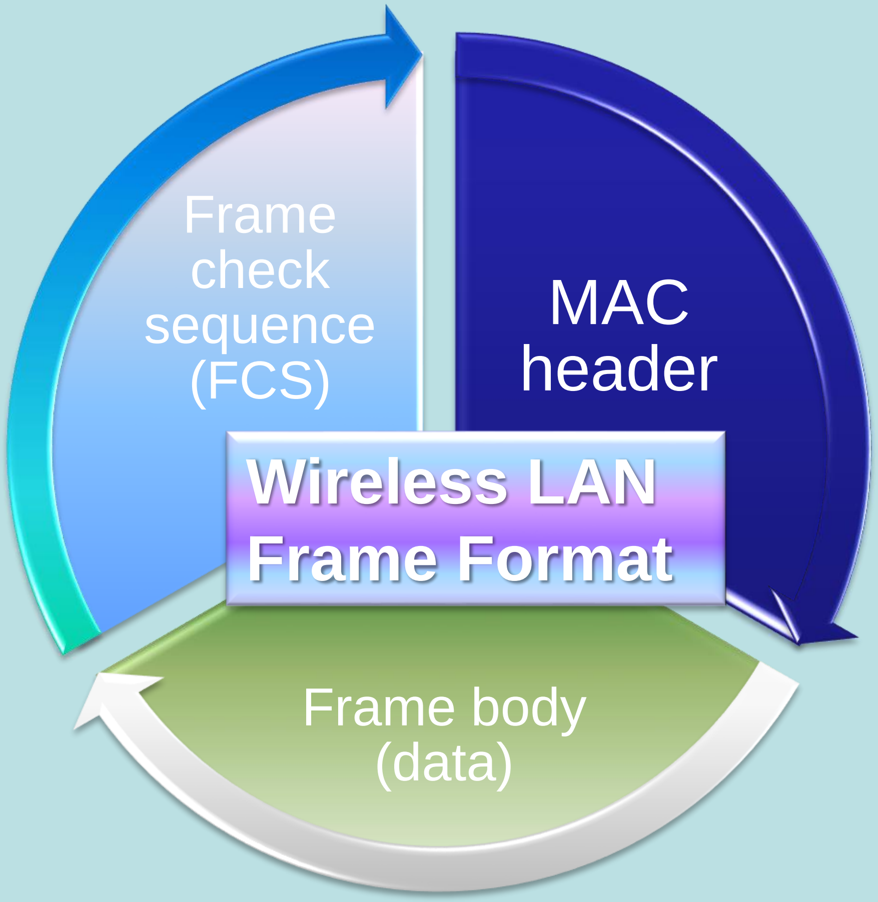
Frame Format

- Three sections in WLAN frame format
- 1. A MAC header
- 2. Variable length frame body – data
- 3. Frame check sequence (FCS) using 32-bit CRC – error detection



Octets: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

MAC Header

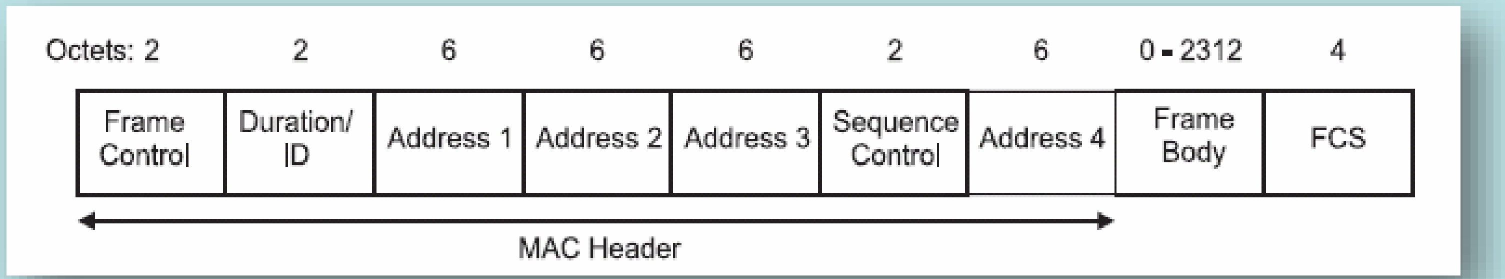


Wireless LAN Frame Format

MAC header

Frame body (data)

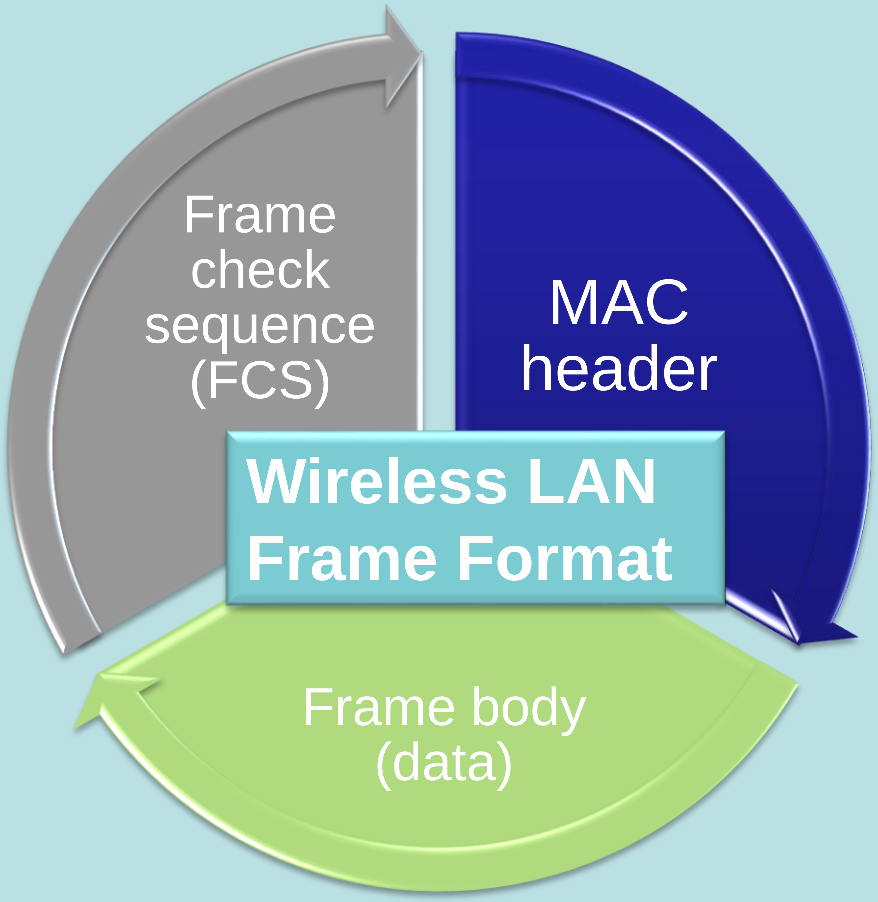
Frame check sequence (FCS)

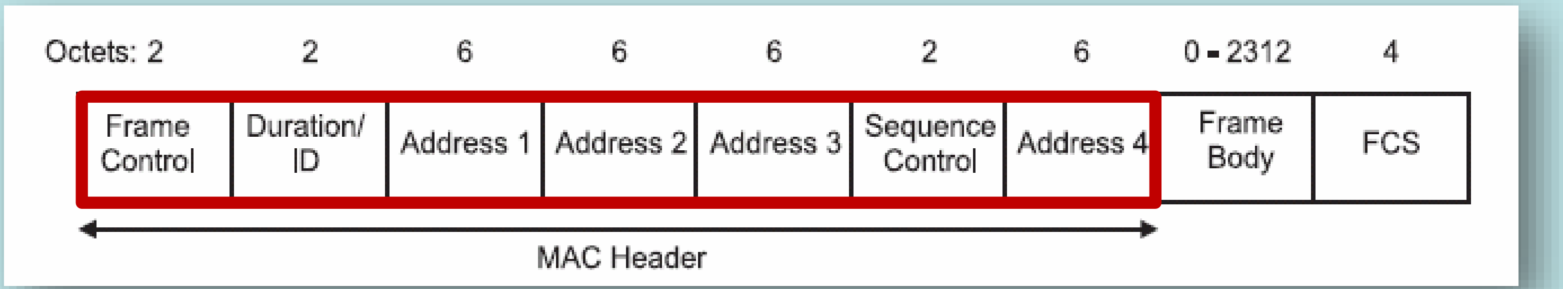


Octets: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

MAC Header

Wireless LAN Frame Format

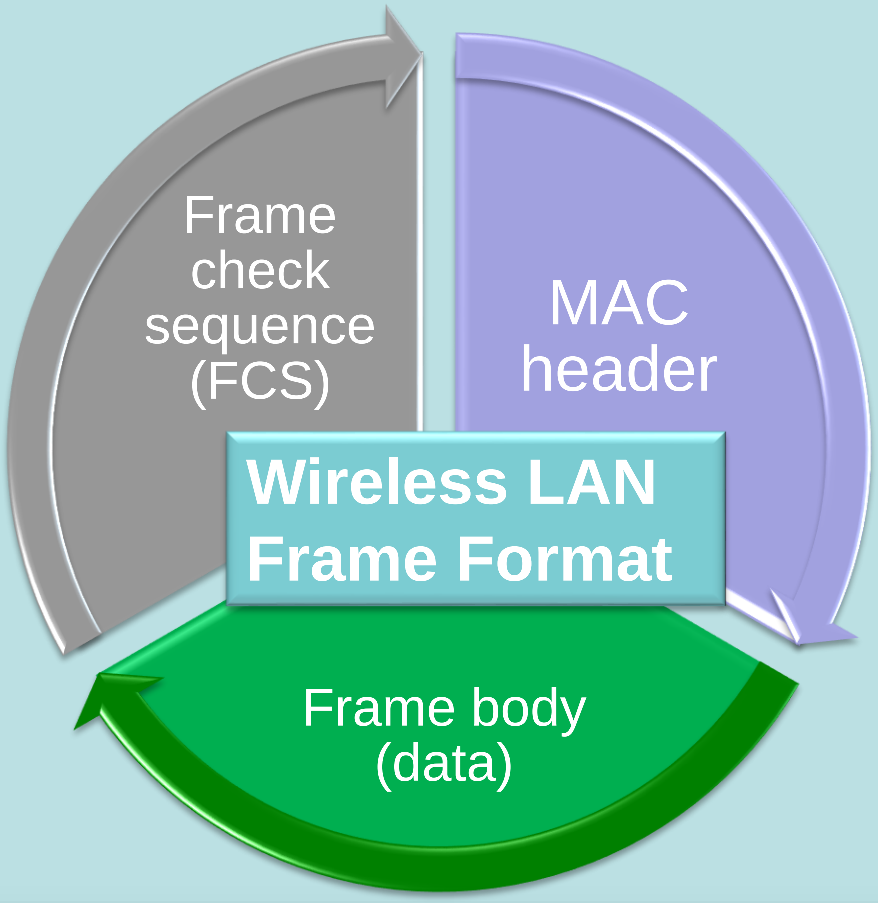


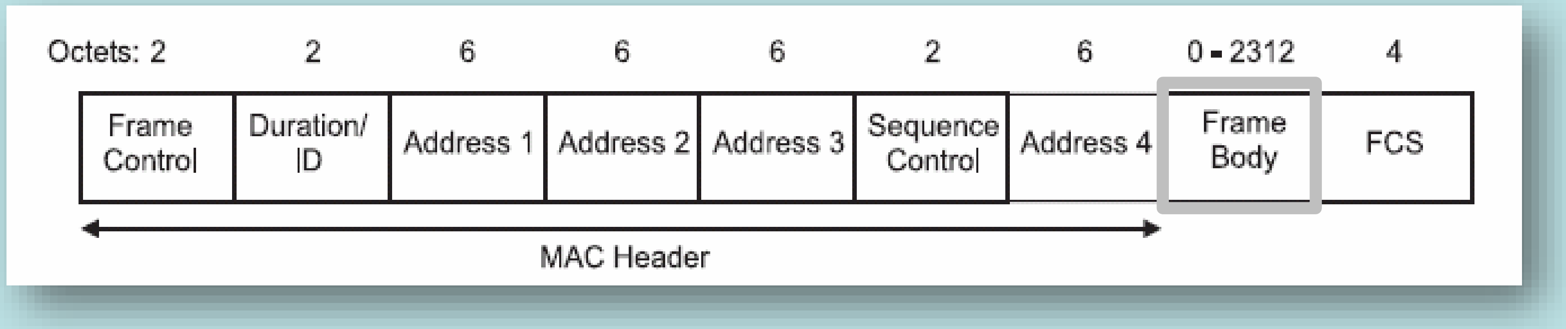


Octets: 2	2	6	6	6	2	6	0 – 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

MAC Header

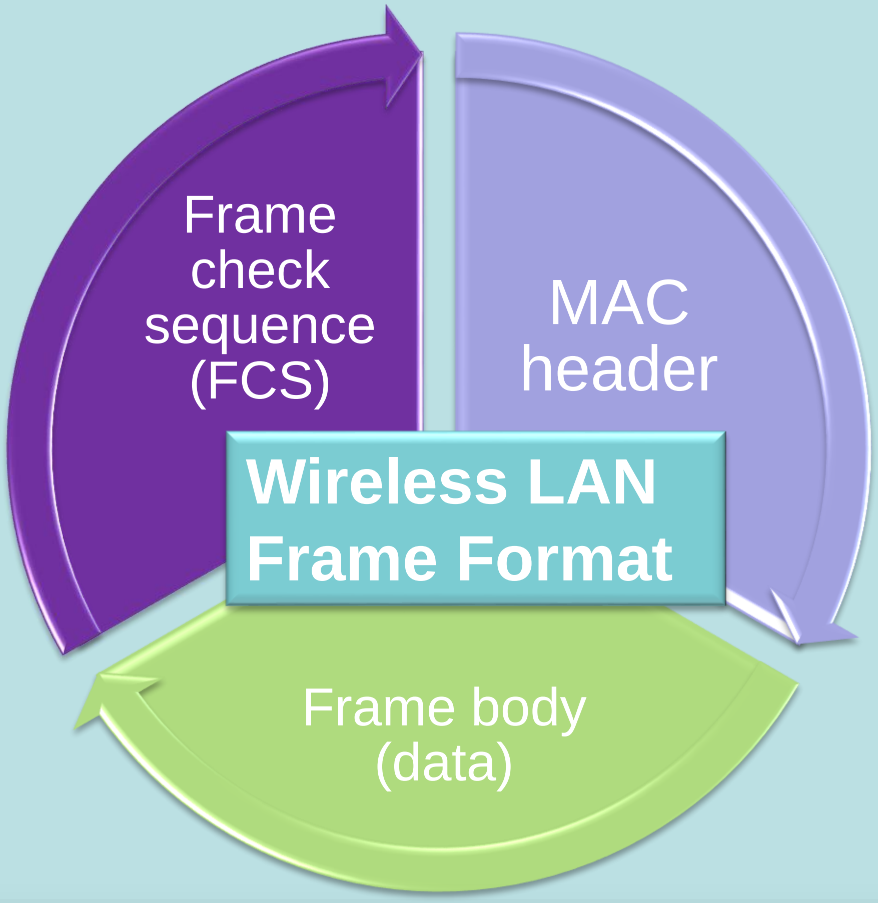
Wireless LAN Frame Format





Octets: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

MAC Header

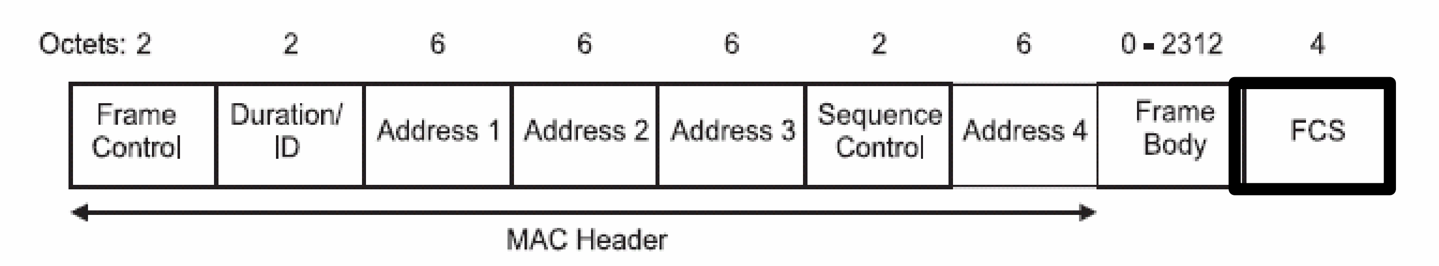


Wireless LAN Frame Format

MAC header

Frame body (data)

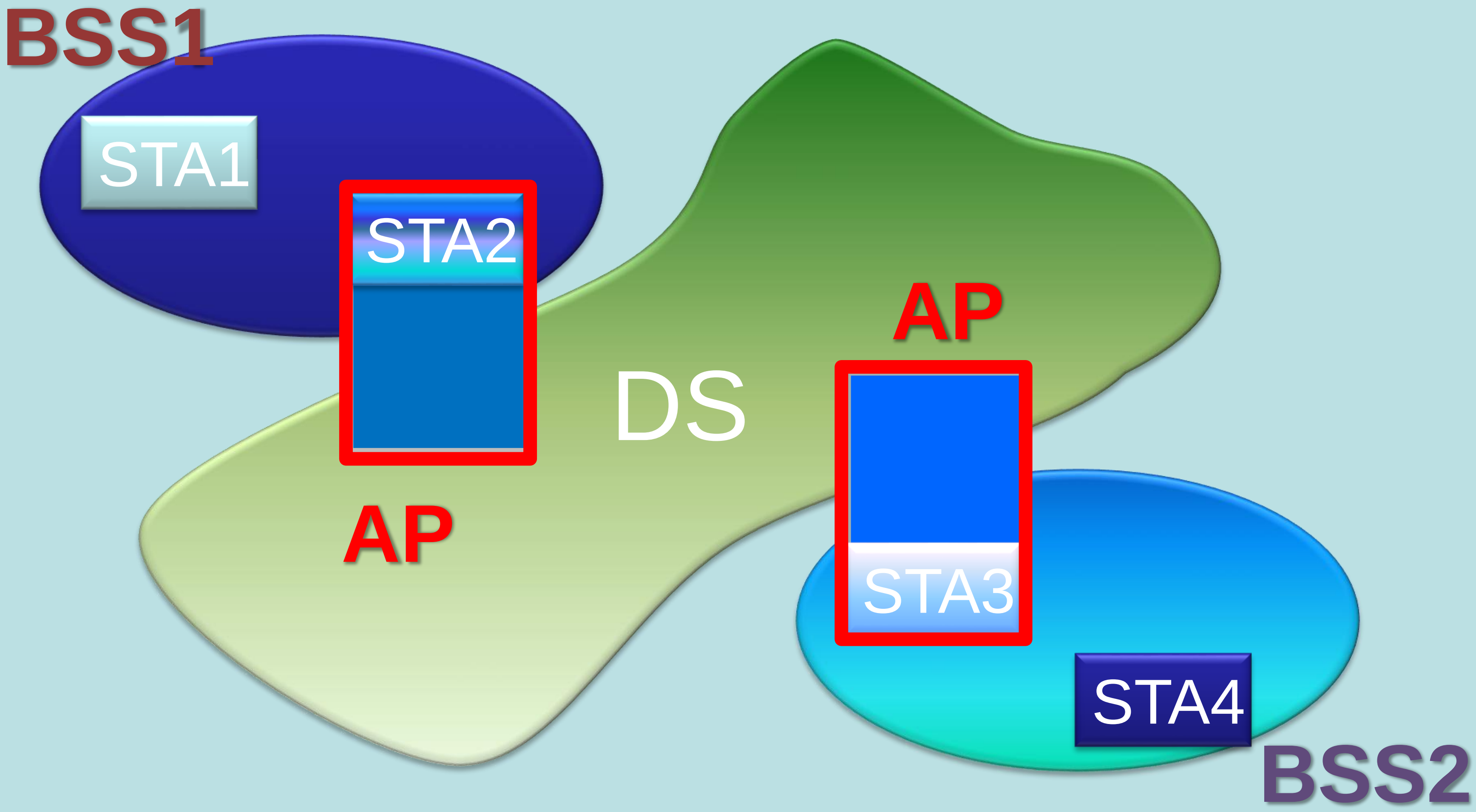
Frame check sequence (FCS)



Octets: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

MAC Header

Remember the ESS?

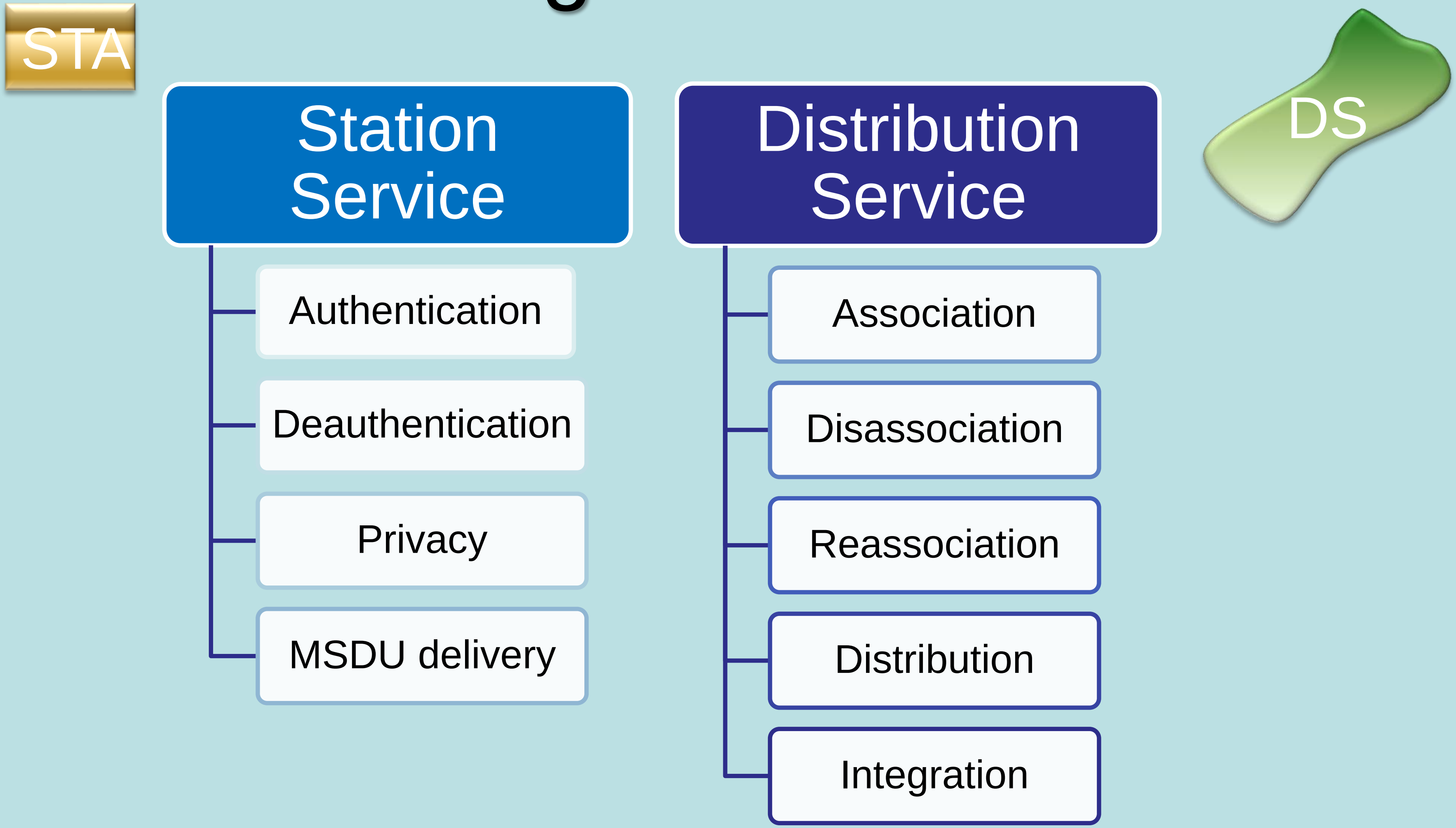


Official (Open), Non-sensitive

Logical Services

- Defined in the standards to allow the equipment vendors to implement as they see fit

9 Logical Services



STA

Station Service

- Authentication
- Deauthentication
- Privacy
- MSDU delivery

Distribution Service

- Association
- Disassociation
- Reassociation
- Distribution
- Integration

DS

Distribution Service

Distribution Service

- Route frames from input to DS (AP) to output from DS (AP) based on information provided to DS by the three association related services
- Integration Service
- If output from DS is wired LAN, it is responsible for accomplishing whatever is needed to deliver frames to the wired LAN

Distribution Service

Association Service

- Provides STA to AP mapping to the DS
- Association is always initiated by STA, not the AP
- Association Request subtype packet
- The AP will respond with a Management type, Association Response subtype packet
- Association Response subtype packet contains capability information, Status code, AID and supported rates

Distribution Service

Reassociation Service

- move current association from one AP to another when STA is roaming
- Reassociation is always initiated by STA, not the AP
- STA to new AP using Management, Reassociation Req
- New AP to STA using Management Reassociation Res

Distribution Service

Dissociation Service

- Terminate an existing association
- STA or AP can invoked this service using Management, Disassociation

Station Service

Authentication Service

- Establish STA identity with one another at the link level using Management, Authentication
- Open System Authentication authenticates any STA
- Shared Key Authentication uses WEP
- Information exchange between STAs
  - Authentication algorithm identification
  - Station identity assertion
  - Authentication transaction sequence number
  - Authentication algorithm dependent information

Station Service

Deauthentication Service

- Terminate an existing authentication
- STA or AP can invoked this service using
- Management, Deauthentication sub type packet
- Frame body contain the reason code

Privacy Service

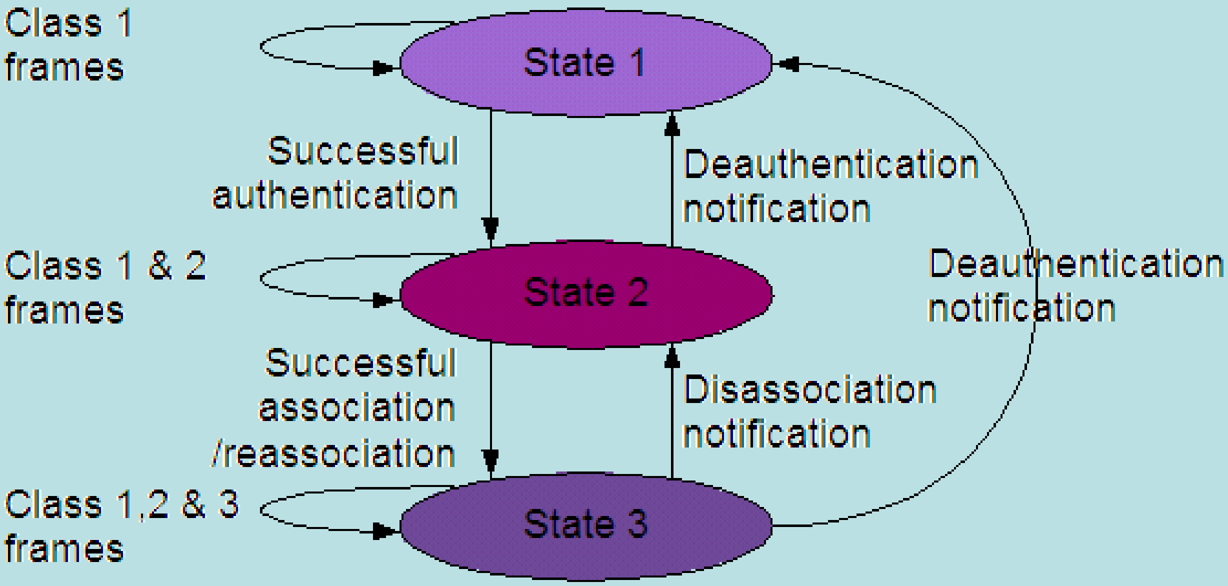
- Encrypt contents using Wired Equivalent Privacy (WEP)

MSDU delivery

- Ensure that the information in the MAC service data unit is delivered between the medium access control service access points

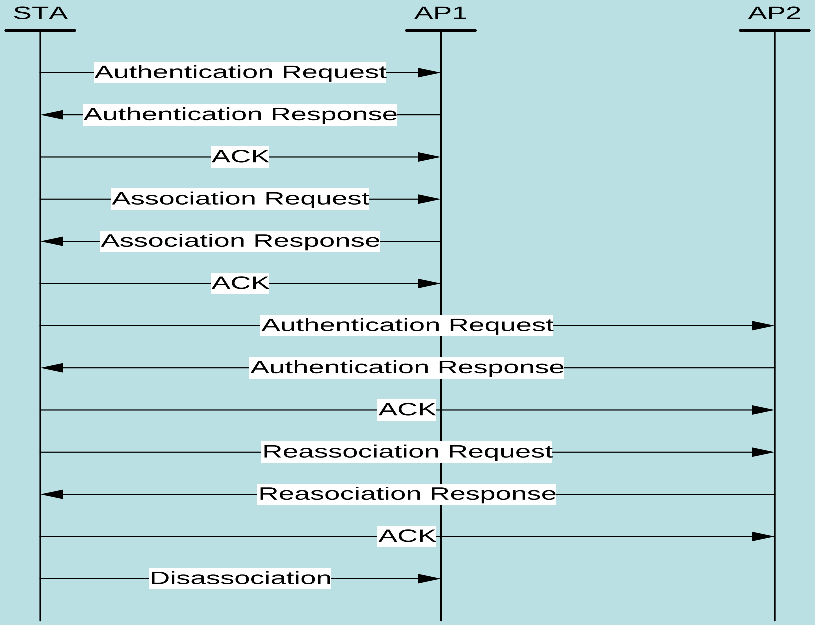
Relationship between services

- State 1 (Initial, unauthenticated, unassociated)
- State 2 (authenticated, unassociated)
- State 3 (authenticated, associated)


Class 1 frames
State 1
Successful authentication
Deauthentication notification
Class 1 & 2 frames
State 2
Deauthentication notification
Successful association /reassociation
Disassociation notification
Class 1,2 & 3 frames
State 3

Example

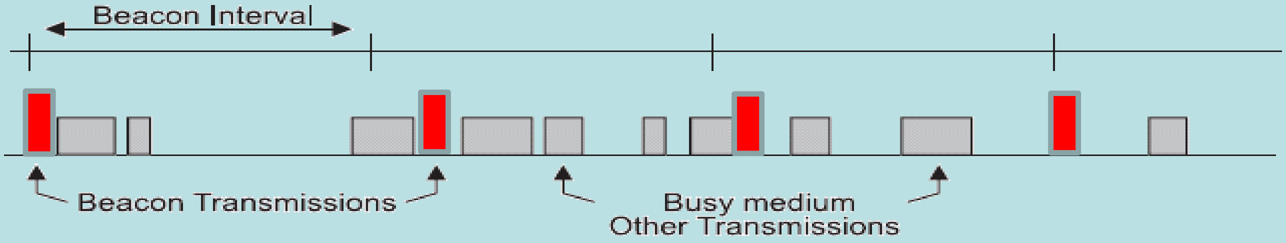
- The exchange of management packets between STA and two APs for authentication, association and reassociation are shown.
- A station moves current association from one AP to another AP when it is roaming



Official (Open), Non-sensitive

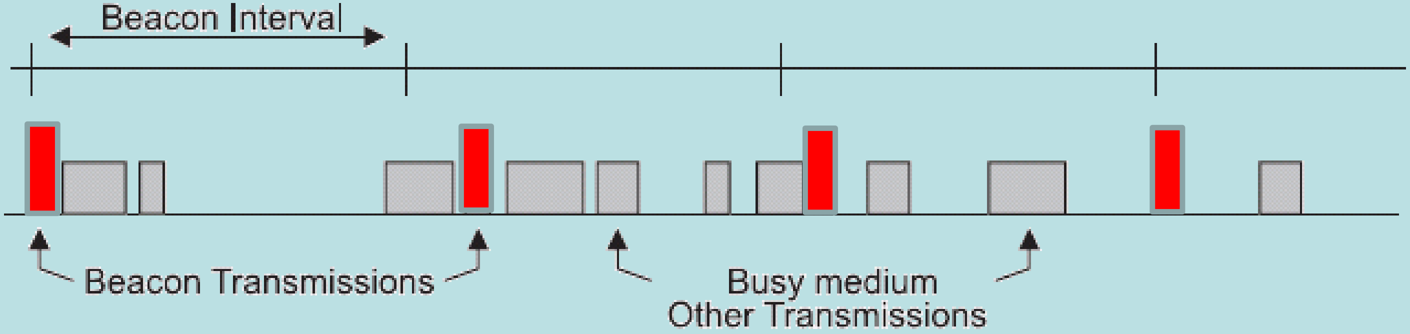
Power Management

- AP sends out a beacon signal/frame that contains a timestamp to all STAs at regular intervals
- When the STAs receive this frame from the AP, they synchronise their local timers with that of the AP.
- When an STA goes into sleep mode, the AP is informed of the change.
- The AP has a record of those STAs that are awake and those that are sleeping.



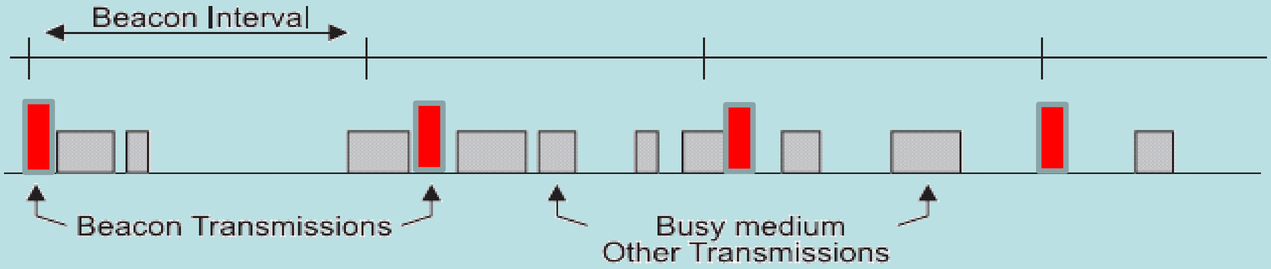
Power Management

- As the AP receives transmissions, it first checks whether the STA is in sleep mode.
- If it is sleeping, the AP temporarily stores (buffers) the synchronised frames.



Power Management

- Beacon frame contains a list, known as the Traffic Indication Map (TIM), of the STAs that have buffered frames waiting at the AP.
- At that same time, all STAs that have been sleeping must awaken and go into an active listening mode.
- If the STA learns that it has buffered frames waiting, the STA can send a request to the AP for those frames.
- If it has no buffered frames, it can return to sleep mode.



IEEE 802.11 Securities

- Authentication
  - Authentication is a process that verifies that the STA has permission to access the network.
  - In IEEE 802.11 WLAN, a Service Set Identifier (*SSID) of the network has to be configured at all its APs.*
  - *For authentication, a STA can be given an SSID in one of two ways.*
  - *First, the SSID can be manually entered into the STA. Once it is entered, anyone who has access to that STA can see the SSID and freely distribute it.*
  - *The second way is even less secure. APs can freely advertise the SSID to any mobile device that comes into the range of the AP. The default setting on most of the APs is freely broadcast SSIDs.*

IEEE 802.11 Securities

- Authentication
  - *For security measures to protect your network, APs should be configured not to broadcast the SSID.*
  - *Hence, turning off SSID broadcast can protect the network against someone finding it unintentionally.*
  - *When an STA transmits a probe frame, the AP will usually send a response that includes the SSID of the network.*
  - *Beware: An attacker using a sniffing device will also be able to obtain the SSID of the access point as well.*

IEEE 802.11 Securities

- *Privacy*
- *Privacy attempts to ensure that the transmitted data are not read by unauthorised users.*
  - *This is accomplished with data encryption, which scrambles the data in a way that it cannot be read and can only be decoded by the intended recipient.*

IEEE 802.11 Securities

- *Wired Equivalent Privacy (WEP)*
- *The IEEE 802.11 standard provides an optional WEP specification for data encryption between wireless devices to prevent eavesdropping.*
- *WEP encryption comes in two versions: 64-bit encryption is actually made up of a 40-bit key (5 bytes or 10 hexadecimal digits) plus a 24 –bit initialisation vector (IV), which is a part of the encryption key that sent in **clear text**, before the encrypted data.*
- *Likewise, 128-bit encryption is made up of a 104-bit key plus a 24-bit IV. Some vendors offered 256-bit encryption in their product; however, this equipment also uses the same 24-bit IV.*
- *256-bit encryption may not be compatible between products from different manufacturers.*

IEEE 802.11 Securities

- ***Wi-Fi Protected Access (WPA)***
- *WPA is a standard for network authentication and encryption introduced by the Wi-Fi Alliance, in response to the **weakness in WEP** described in the previous section.*
- *WPA uses 128-bit pre-shared keys (PSK), which is also called personal mode. WPA-PSK uses a different encryption key for each client device, for each packet, for each session, unlike WEP, which only varies the 24-bit IV.*
- *WPA employs the temporal key integrity protocol (TKIP), which provide per-packet key-mixing. In addition, TKIP also provides message integrity check (MIC), which uses a combination of variable and static items, such as the current network uptime or the value of a continually incrementing variable and other data items to ensure that the encrypted data has not been tampered with.*
- *TKIP uses a 48-bit hashed initialization vector and also changes the key after a user-specified amount of time.*

WLAN Applications

- WLAN is used primarily for web browsing and e-mail.
- WLAN networks are now being tasked to support more demanding applications such as video surveillance, video conferencing and voice over IP (VoIP) services.
- *Doctors and nurses in hospitals* are more productive because hand-held or notebook computers with wireless LAN capability deliver patient information instantly.
- *Consulting or accounting audit engagement teams* or small workgroups increase productivity with quick network setup.

WLAN Applications

- *Network managers in dynamic environments* minimize the overhead of moves, adds, and changes with wireless LANs, thereby reducing the cost of LAN ownership.
- *Training sites at corporations and students at universities* use wireless connectivity to facilitate access to information, information exchanges, and learning.
- *Network managers installing networked computers in older buildings* find that wireless LANs are a cost-effective network infrastructure solution.
- *Retail store owners* use wireless networks to simply frequent network reconfiguration.

WLAN Applications

- *Trade show and branch office workers* minimize setup requirements by installing preconfigured wireless LANs needing no local MIS support.
- *Warehouse workers* use wireless LANs to exchange information with central databases and increase their productivity.
- Network managers implement wireless LANs to provide *backup for mission-critical applications* running on wired networks.
- *Senior executives in conference rooms* make quicker decisions because they have real-time information at their fingertips.

Advantages of WLANs

- **Mobility**-Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
- **Installation -** Speed and Simplicity-Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- Installation **Flexibility**-Wireless technology allows the network to go where wire cannot go.

Advantages of WLANs

- **Reduced Cost**-of-Ownership-While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, adds, and changes.
- **Scalability**-Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that allows roaming over a broad area.

Summary

1. MAC Functional Operation
2. Frame Format
3. Logical Services
4. Power Management
5. IEEE 802.11 Securities
6. Examples of WLAN Applications
7. Advantages of WLANs