ITSC 301: Wireless Security

Module 4 – Wireless Layer 2 Technology

Table of Contents

- Review lecture and lab
- Explain wireless LAN frame structure
- Define terms used in 802.11 layer 2 technology
- Examine common capabilities of the IEEE 802.11 MAC
- Use tools to analyze layer 2 wireless traffic
- Troubleshoot wireless LAN connectivity problems by interpreting the layer 2 frame

Review Lecture & Lab

Review

- Antennas
- Spread Spectrum
- Encoding
- Modulation
- Multiplex

Wireless
Layer 2

Learning Objectives

- Explain the functions of the standard components of a WLAN frame (Data, Control and Management frames)
- Define terms used in 802.11 layer 2 technology: DCF, CSMA/CA, RTS/CTS, DRS and WMM
- Examine common capabilities of the IEEE 802.11 MAC
- Use tools to analyze layer-2 wireless traffic (lab)
- Troubleshoot wireless LAN connectivity problems by interpreting the layer-2 frame (lab)

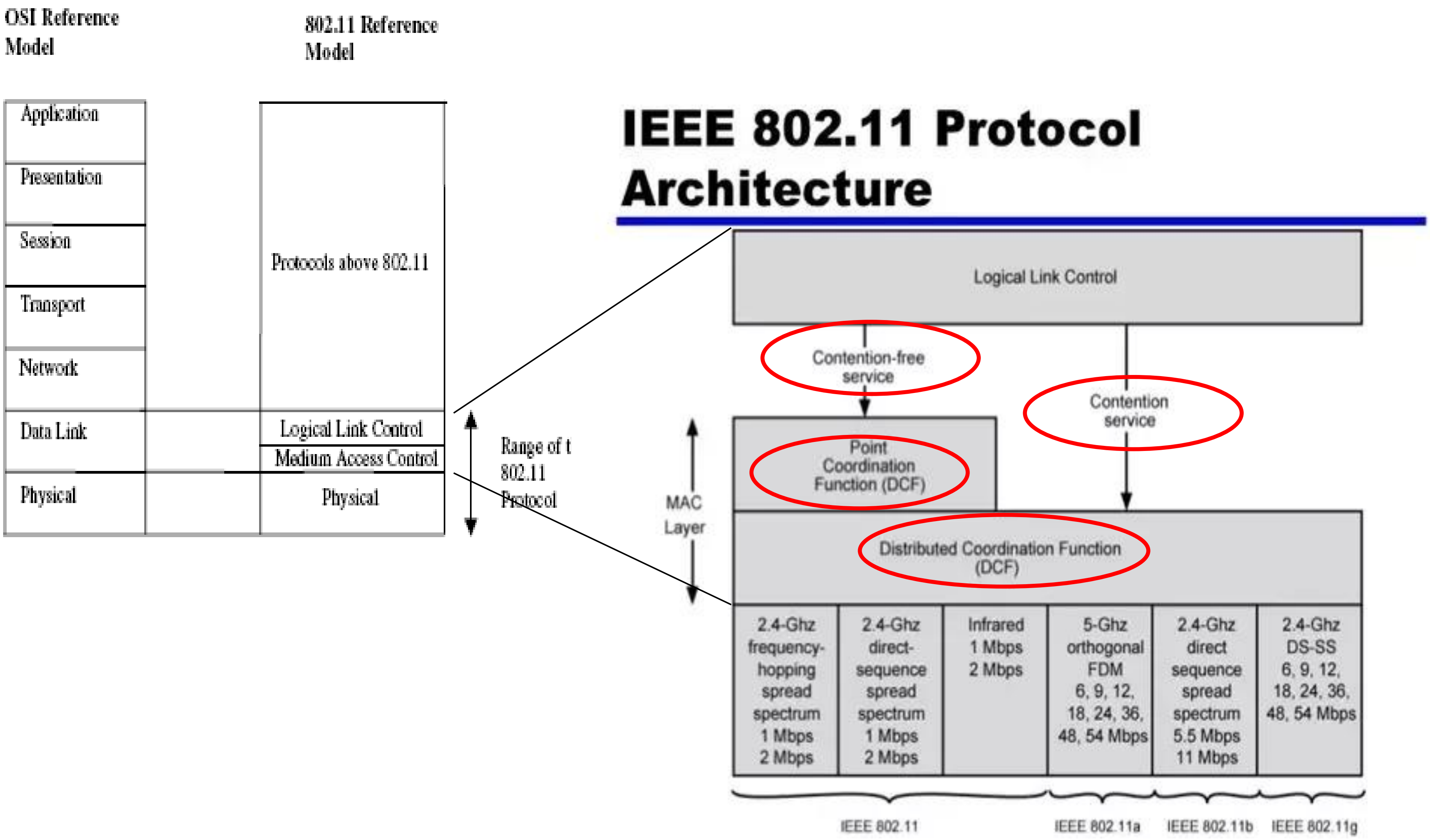
Small Group Discussion

- Investigate the functions of the standard components of a Wireless LAN frame (Data, Control and Management frames)

Physical Layer Wireless (802.11)

- Remember Module 2
  - Dispersion, refraction, reflection, diffraction, absorption, scatter
- 802.11 physical layer unreliable
  - Noise, interference and other propagation effects result in loss of frames
  - Even with error-correction codes, frames may not be successfully received

OSI Model & 802.11 MAC/LLC Layer



OSI Reference Model

802.11 Reference Model

Application

Presentation

Session

Transport

Network

Data Link

Physical

Protocols above 802.11

Logical Link Control

Medium Access Control

Physical

Range of t 802.11 Protocol

IEEE 802.11 Protocol Architecture

Logical Link Control

Contention-free service

Contention service

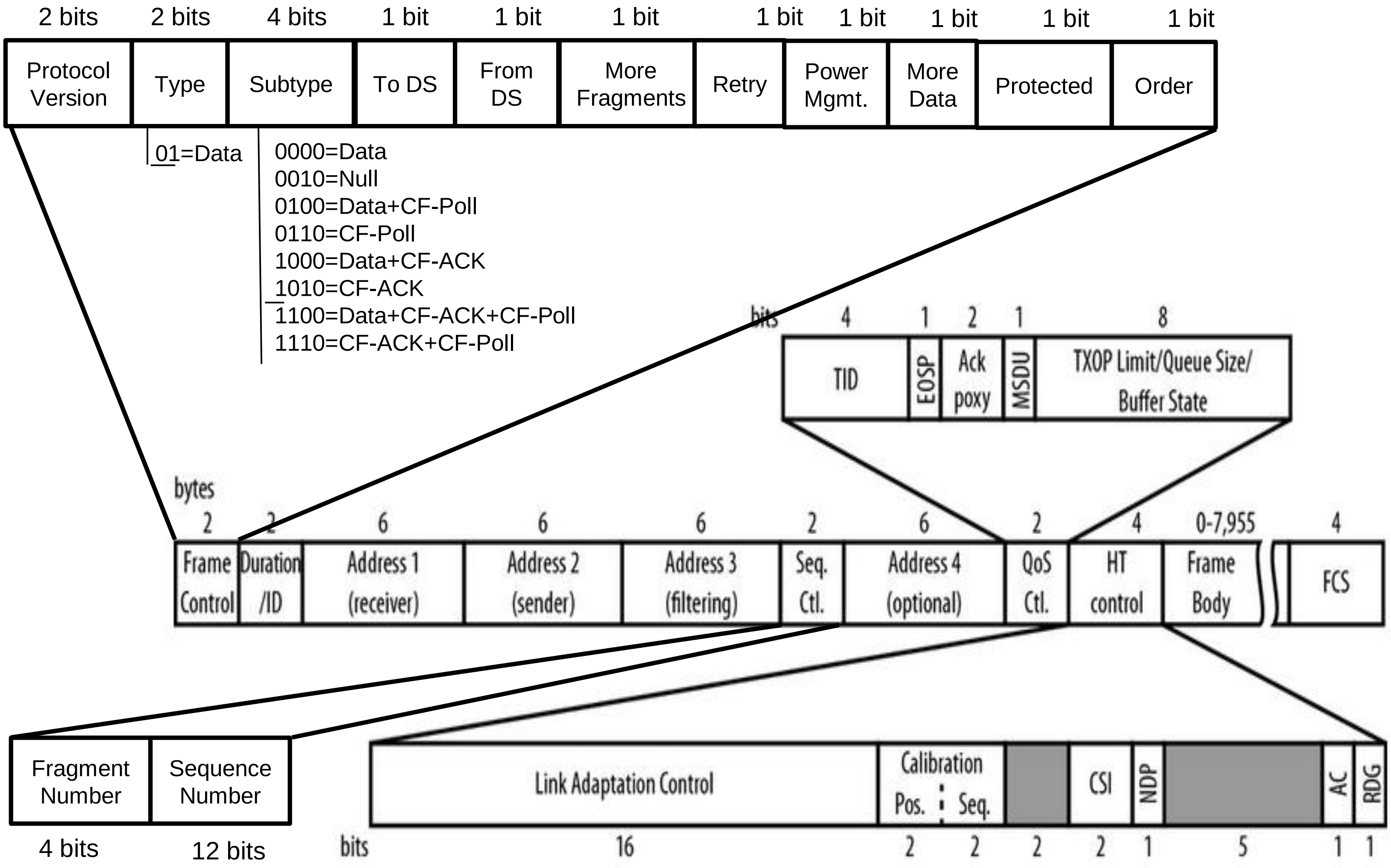
Point Coordination Function (DCF)

MAC Layer

Distributed Coordination Function (DCF)

2.4-Ghz frequency-hopping spread spectrum 1 Mbps 2 Mbps	2.4-Ghz direct-sequence spread spectrum 1 Mbps 2 Mbps	Infrared 1 Mbps 2 Mbps	5-Ghz orthogonal FDM 6, 9, 12, 18, 24, 36, 48, 54 Mbps	2.4-Ghz direct sequence spread spectrum 5.5 Mbps 11 Mbps	2.4-Ghz DS-SS 6, 9, 12, 18, 24, 36, 48, 54 Mbps
IEEE 802.11			IEEE 802.11a	IEEE 802.11b	IEEE 802.11g

MAC Frame on Wireless (802.11)



2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgmt.	More Data	Protected	Order

01=Data

0000=Data
0010=Null
0100=Data+CF-Poll
0110=CF-Poll
1000=Data+CF-ACK
1010=CF-ACK
1100=Data+CF-ACK+CF-Poll
1110=CF-ACK+CF-Poll

Fragment Number	Sequence Number
4 bits	12 bits

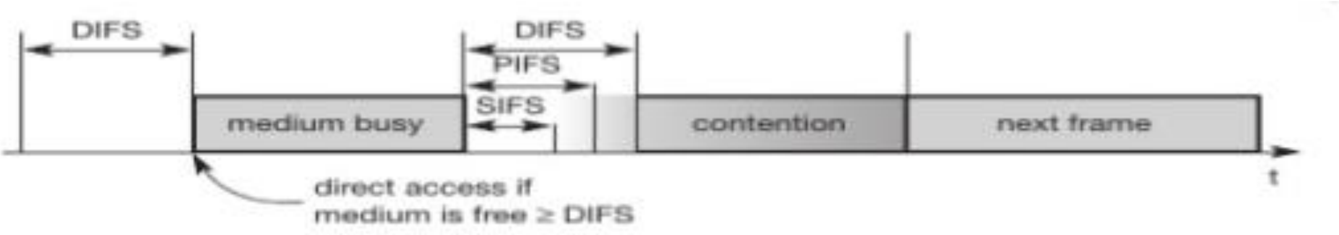
Figure 2: title

Adapted from netprojnetworks, 2017. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

802.11 Medium Access Control Terms

- Asynchronous data service (DCF)
  - Collision Sense Medium Access / Collision Avoidance (CSMA/CA)
  - Return to Sender / Call to Sender (RTS/CTS)
- Time-bound service (PCF)
  - Polling
- Inter-frame spacing (IFS)
  - Distributed coordinated function IFS (DIFS)
  - Point coordinated IFS (PIFS)
  - Short IFS (SIFS)
- Fragmentation

802.11 MAC Definitions



- **Short inter-frame spacing (SIFS)** – shortest waiting for medium access (highest priority) ex. Control msg.
- **PCF inter-frame spacing (PIFS)** – used for time bounded services.
- **DCF inter-frame spacing (DCF)** – longest waiting time and has the lowest priority for medium access.

[Contention – duration in which several nodes try to access the medium]

Figure 3: Medium Access and Inter-Frame Spacing

Source: Hada, R., 2013. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

802.11 MAC Contention

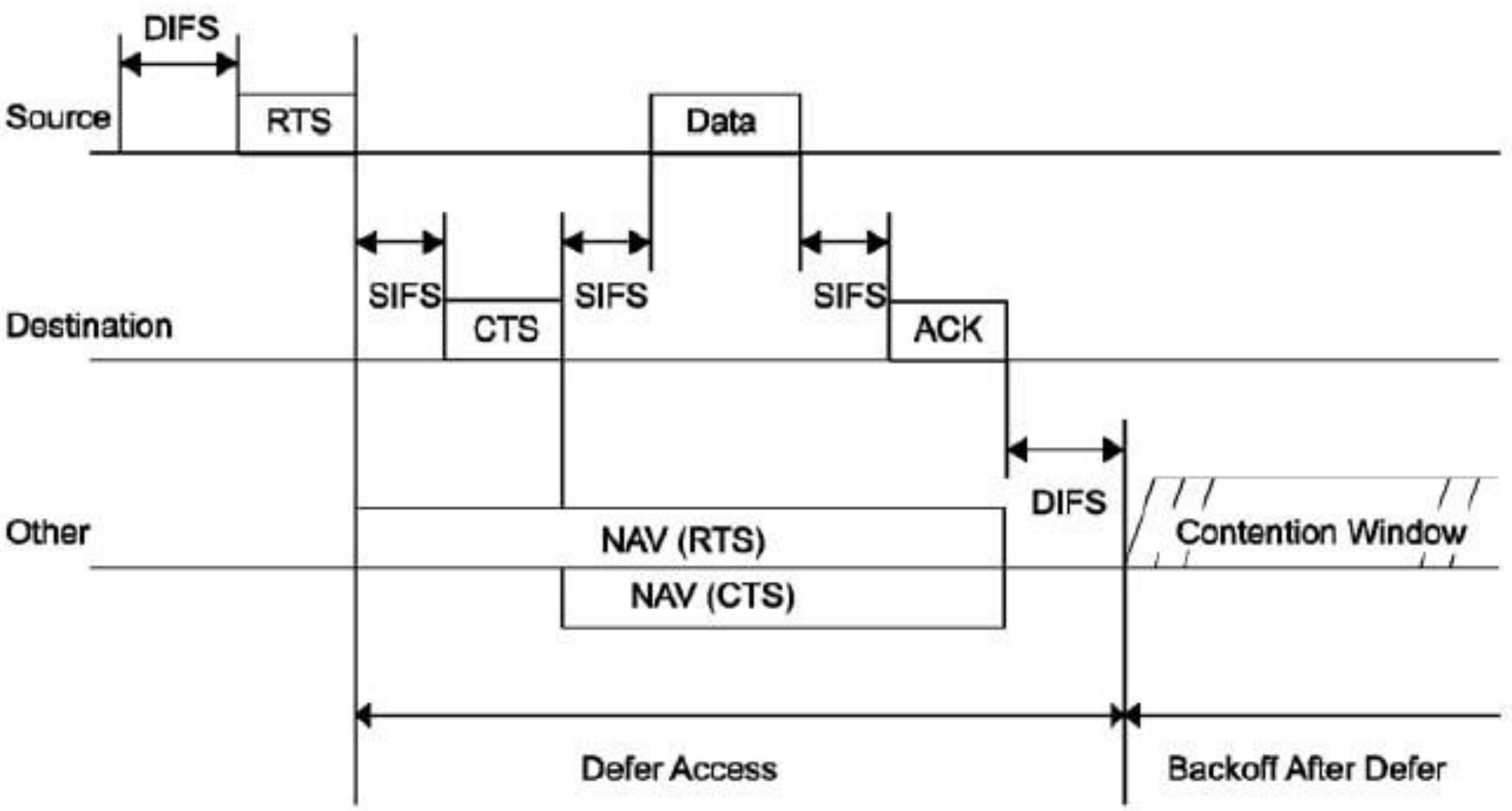


Figure 4: title
Source: Sarker, M., 2017. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

802.11 MAC Definitions

- The DCP scheme is refined to provide priority-based access using three values for IFS:
  - DIFS - The longest IFS, used as a minimum delay for a synchronous frames contending for access
    - Used for all ordinary asynchronous traffic
  - PIFS - A mid-length IFS
    - Used by the centralized controller in issuing polls
    - Takes precedence over normal contention traffic

802.11 MAC Definitions - SIFS

- Used for all immediate response actions
- Any station using SIFS to determine transmission opportunity has the highest priority, because it will always gain access in preference to a station waiting an amount of time equal to PIFS or DIFS.
- Used in the following circumstances:
  - Acknowledgment (ACK)
  - Clear to Send (CTS)
  - Poll response

Media Access Control (MAC)

- Time Bound Service – Point Coordinator Frame (PCF)
  - Alternative access method implemented on top of the DCF
  - Operation consists of polling by the centralized polling master (point coordinator)
  - Point coordinator makes use of PIFS when issuing polls
  - PIFS is smaller than DIFS
    - Point coordinator can seize the medium and lock out all asynchronous traffic while it issues polls and receives responses

Media Access Control (MAC)

- Time Bound Service – PCF (continued)
  - Stations with time-sensitive traffic are controlled by the point coordinator while remaining traffic contends for access using CSMA
  - Interval known as the super frame is defined
  - During the first part of interval, point coordinator issues polls in a round-robin fashion to all stations configured for polling
  - The point coordinator then idles for the remainder of the super frame, allowing a contention period for asynchronous access

(Hong, 2004)

802.11 MAC Definitions: PCF Mode

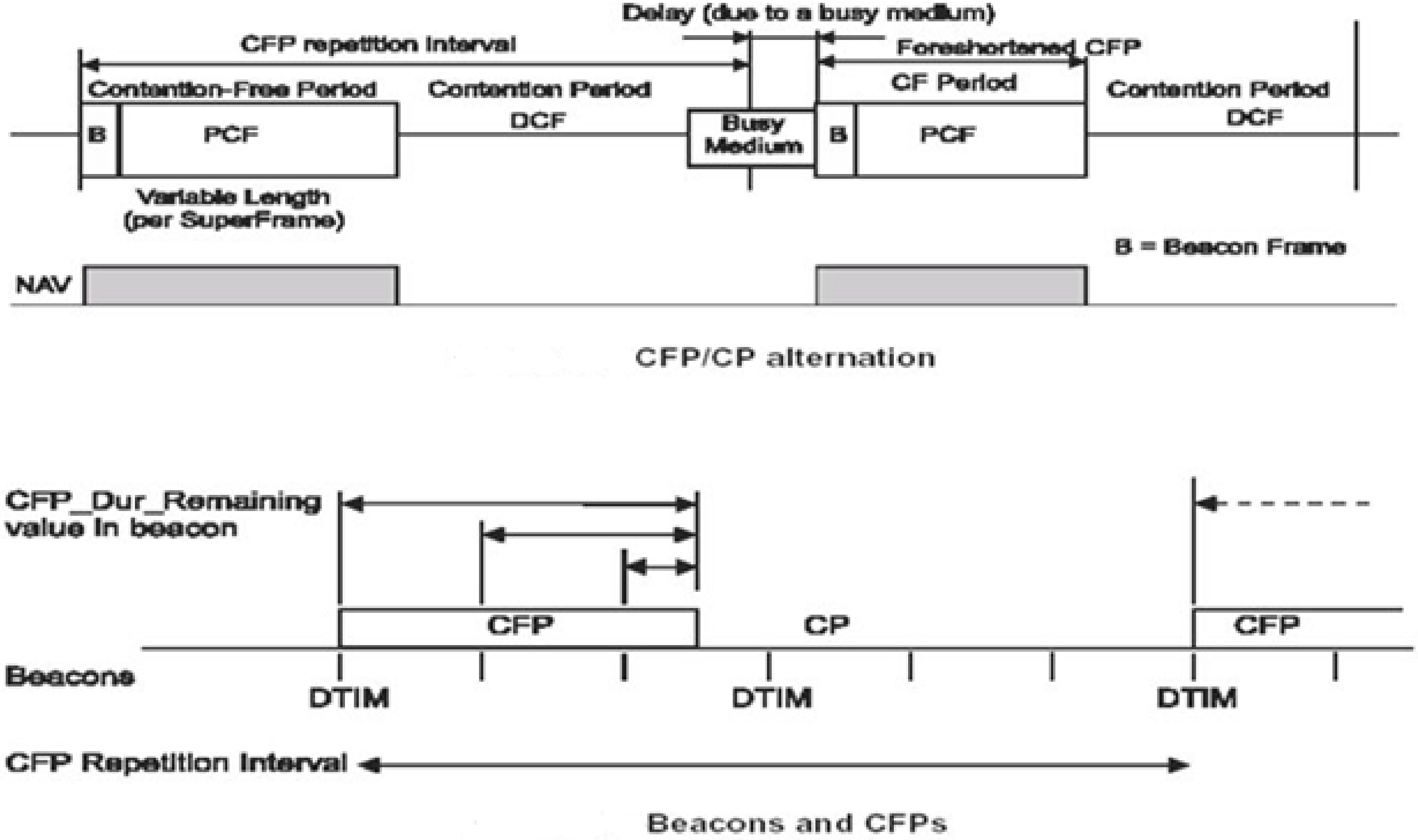


Figure 5: PCF Mode

Source: Goliya, A., 2003. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

802.11 MAC Definitions: Fragmentation

- Wireless LANs can have high bit error rates
- Probability of frame errors much higher for wireless links
- 802.11 uses fragmentation to reduce the frame error rate

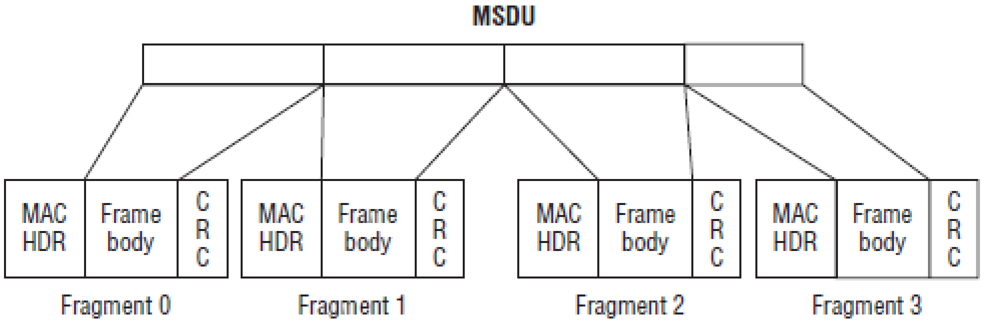


Figure 6: Fragmentation of an MSDU
Source: Nayanajith, R., 2014. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

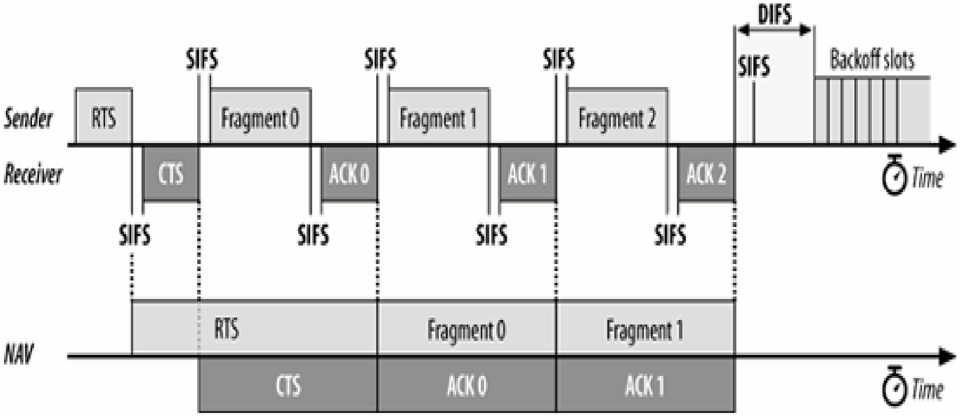
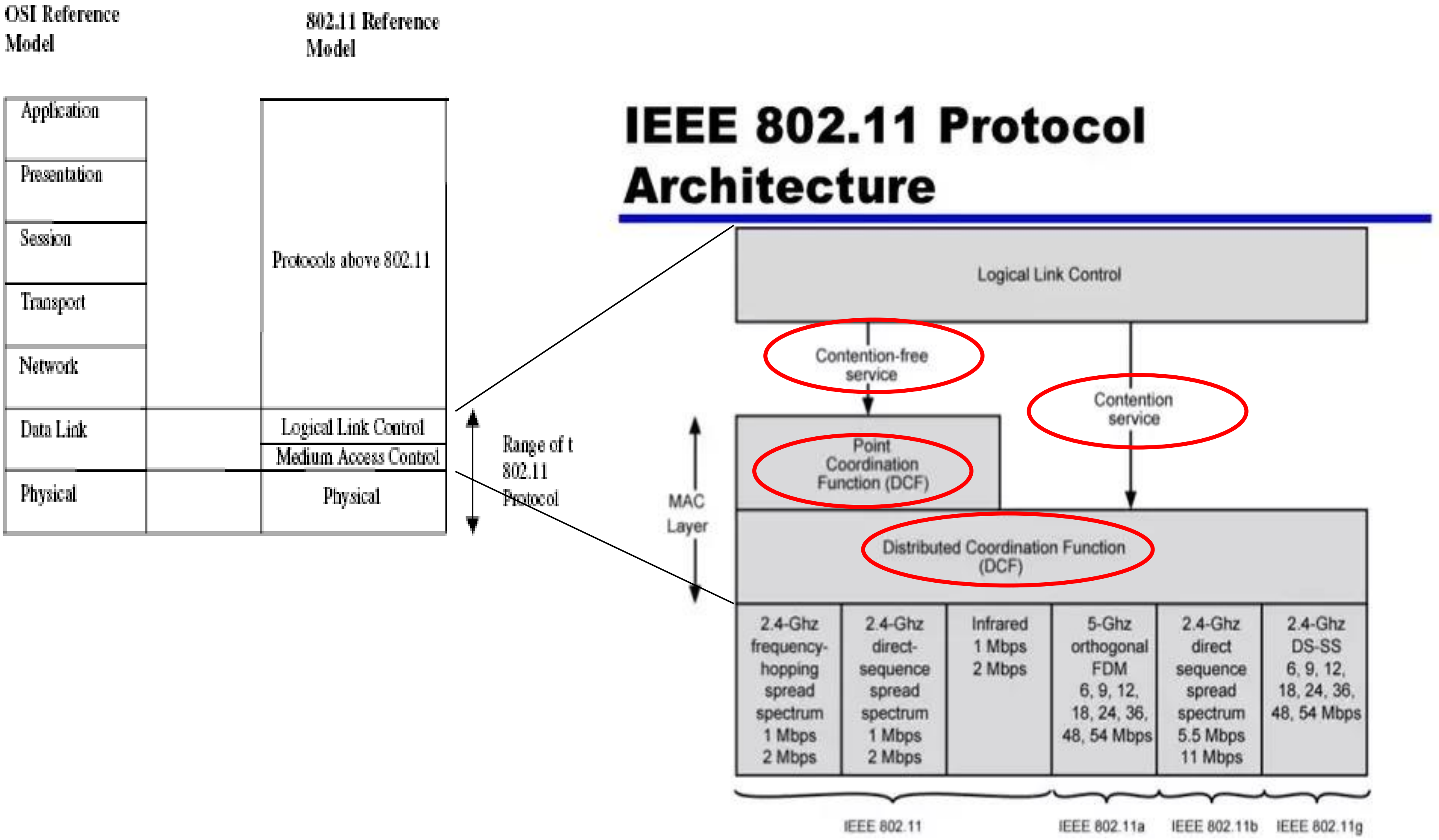


Figure 7: title
Source: ???. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

OSI Model & 802.11 MAC/LLC Layer


OSI Reference Model
802.11 Reference Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
Protocols above 802.11
Logical Link Control
Medium Access Control
Physical
Range of t 802.11 Protocol
IEEE 802.11 Protocol Architecture
Logical Link Control
Contention-free service
Contention service
Point Coordination Function (DCF)
Distributed Coordination Function (DCF)
MAC Layer
2.4-Ghz frequency-hopping spread spectrum 1 Mbps 2 Mbps
2.4-Ghz direct-sequence spread spectrum 1 Mbps 2 Mbps
Infrared 1 Mbps 2 Mbps
5-Ghz orthogonal FDM 6, 9, 12, 18, 24, 36, 48, 54 Mbps
2.4-Ghz direct sequence spread spectrum 5.5 Mbps 11 Mbps
2.4-Ghz DS-SS 6, 9, 12, 18, 24, 36, 48, 54 Mbps
IEEE 802.11
IEEE 802.11a
IEEE 802.11b
IEEE 802.11g

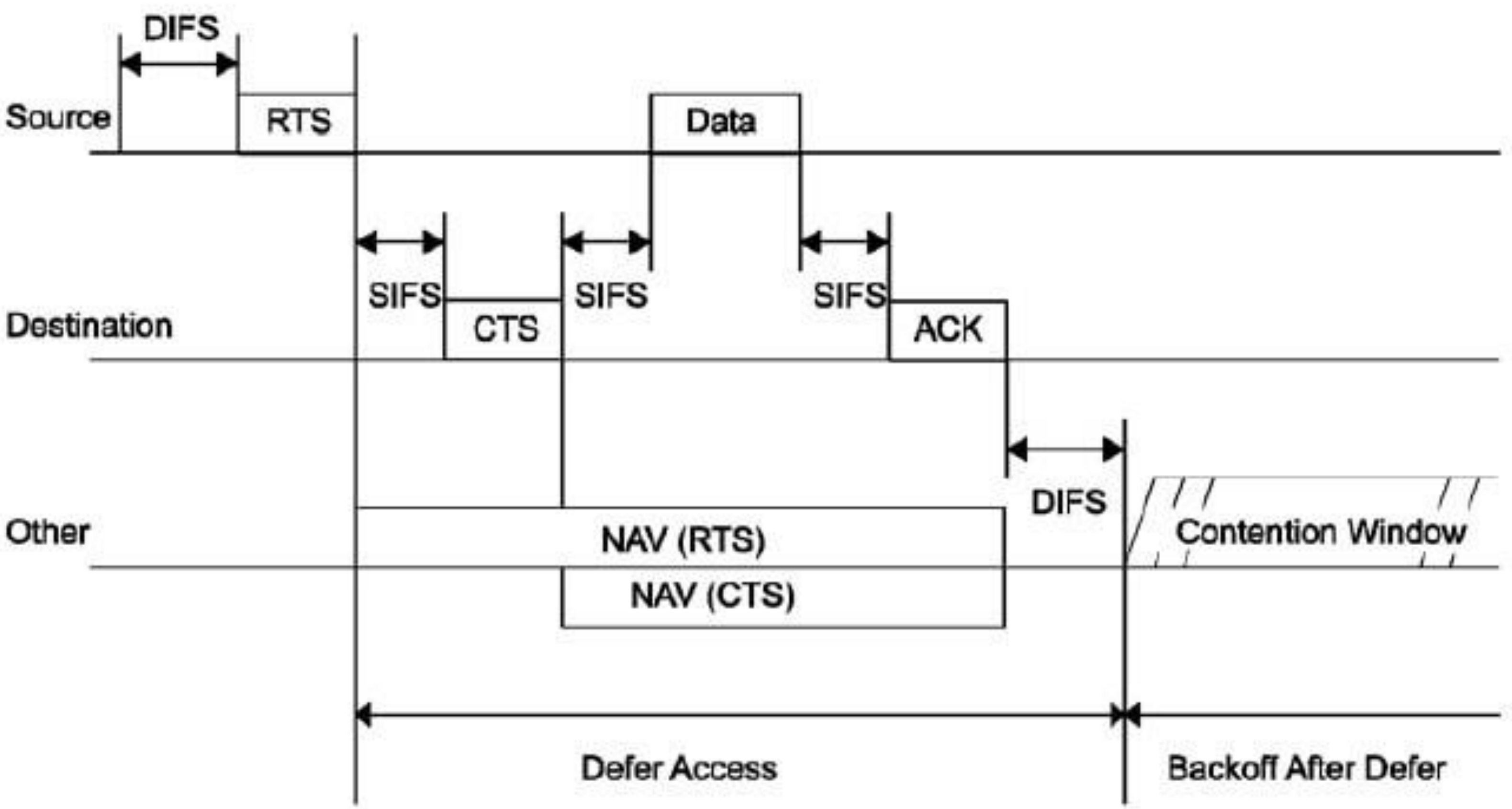
802.11 MAC Data Frame Types

Frame type	Contention-based service	Contention-free service	Carries data	Does not carry data
Data	✓		✓	
Data+CF-Ack		✓	✓	
Data+CF-Poll		AP only	✓	
Data+CF-Ack+CF-Poll		AP only	✓	
Null	✓	✓		✓
CF-Ack		✓		✓
CF-Poll		AP only		✓
CF-Ack+CF-Poll		AP only		✓
https://www.safaribooksonline.com/library/view/80211-wireless-networks/0596100523/ch04.html				

802.11 Media Access Control (MAC)

- IEEE 802.11 includes a frame exchange protocol
  - When a station receives a data frame from another station, it returns an acknowledgment (ACK) frame to the source station
  - If the source does not receive an ACK within a short period of time (data frame damaged or returning ACK damaged), the source retransmits the frame

802.11 MAC Contention



802.11 MAC

- Use four-frame exchange for better reliability
  - A source first issues a Request to Send (RTS) frame to the destination. The destination then responds with a Clear to Send (CTS).
  - After receiving the CTS, the source transmits the data frame, and the destination responds with an ACK.
  - RTS alerts all stations within reception range of the source that an exchange is underway. These stations refrain from transmission in order to avoid a collision between two frames transmitted at the same time
  - CTS alerts all stations that are within reception range of the destination that an exchange is underway.

(Habbani, 2004)

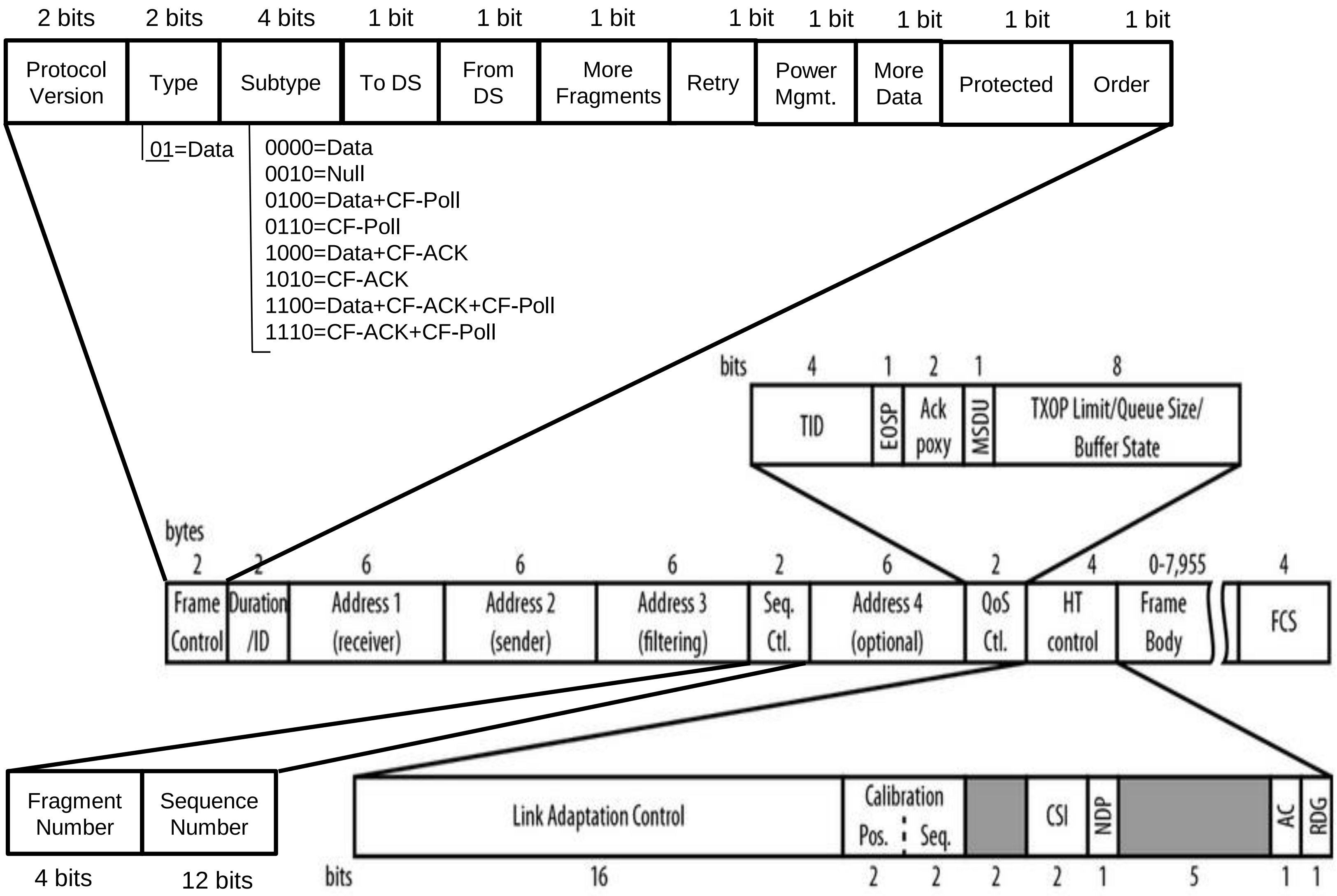
802.11 MAC

- For access control
  - Distributed access protocols, distribute the decision to transmit over all the nodes using a carrier sense mechanism
  - centralized access protocols, which involve regulation of transmission by a centralized decision maker
- MAC algorithm distributed foundation wireless MAC (DFWMAC) provides a distributed access control mechanism with an optional centralized control built on top

Analyze Packet Framing on Wireless

- Dissect Frame

MAC Frame on Wireless (802.11)



2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgmt.	More Data	Protected	Order

01=Data

0000=Data
0010=Null
0100=Data+CF-Poll
0110=CF-Poll
1000=Data+CF-ACK
1010=CF-ACK
1100=Data+CF-ACK+CF-Poll
1110=CF-ACK+CF-Poll

bits	4	1	2	1	8
	TID	EOSP	Ack poxy	MSDU	TXOP Limit/Queue Size/ Buffer State

bytes	2	2	6	6	6	2	6	2	4	0-7,955	4
	Frame Control	Duration /ID	Address 1 (receiver)	Address 2 (sender)	Address 3 (filtering)	Seq. Ctl.	Address 4 (optional)	QoS Ctl.	HT control	Frame Body	FCS

Fragment Number	Sequence Number
4 bits	12 bits

	Link Adaptation Control	Calibration Pos.	Calibration Seq.		CSI	NDP		AC	RDG
bits	16	2	2	2	2	1	5	1	1

MAC (802.11)

- The lower sublayer of the MAC layer is the distributed coordination function (DCF)
    - DCF uses a contention algorithm to provide access to all traffic. Ordinary asynchronous traffic uses DCF directly.
    - Point coordination function (PCF) is a centralized MAC algorithm used to provide contention-free service
    - PCF is built on top of DCF and exploits features of DCF to assure access for its users

MAC (802.11)

- The DCF sublayer makes use of a simple CSMA (carrier sense multiple access) algorithm
  - If a station has a MAC frame to transmit, it listens to the medium
  - If the medium is idle, the station may transmit, otherwise it must wait until the current transmission is complete before transmitting
  - DCF includes a collision-avoidance function (i.e., CSMA/CA) because collision detection (CSMA/CD) is not practical on a wireless network

MAC (802.11)

- The dynamic range of the signals on the medium is very large, so that a transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmission.
- To ensure the smooth and fair functioning of this algorithm, DCF includes a set of delays that amounts to a priority scheme known as an interframe space (IFS).

IEEE 802.11 MAC Control Frame

- Control frames assist in the reliable delivery of data frames
- There are six control frame subtypes:

1. Power Save-Poll (PS-Poll): sent by any station to the station that includes the AP (access point) to request that the AP transmit a frame that has been buffered for this station while the station was in power-saving mode.
2. Request to Send (RTS): the first frame in the four-way frame exchange alerting a potential destination, and all other stations within reception range, that it intends to send a data frame to that destination.

IEEE 802.11 MAC Control Frame

3. Clear to Send (CTS): the second frame in the four-way exchange sent by the destination station to the source station to grant permission to send a data frame
4. Acknowledgment: Provides an acknowledgment from the destination to the source that the immediately preceding data, management, or PS-Poll frame was received correctly
5. Contention-Free (CF)-end: Announces the end of a contention-free period
6. CF-End + CF-Ack: Acknowledges the CF-end. This frame ends the contention-free period and releases stations from the restrictions associated with that period

IEEE 802.11 MAC Data Frame Format

- Eight data frame subtypes, organized into two groups.
- The first four subtypes define frames that carry upper-level data from the source station to the destination station.
- The four data-carrying frames are:

1. Data: the simplest data frame, may be used in both a contention period and a contention-free period
2. Data + CF-Ack: May only be sent during a contention-free period, and also acknowledges previously received data
3. Data + CF-Poll: Used by a point coordinator to deliver data to a mobile station and also to request that the mobile station send a data frame that it may have buffered.
4. Data + CF-Ack + CF-Poll: Combines the functions of the Data + CF-Ack and Data + CF-Poll into a single frame

IEEE 802.11 MAC Data Frame Format

- The remaining four subtypes of data frames do not carry any user data.
  - The Null Function data frame used only to carry the power management bit in the frame control field to the AP, to indicate that the station is changing to a low-power operating state.
  - CF-Ack, CF-Poll, CF-Ack+ CF-Poll: have the same functionality as the corresponding data frame subtypes in the preceding list (Data+ CF-Ack, Data+ CF-Poll, Data+ CF-Ack+ CF-Poll) but without the data.

IEEE 802.11 MAC Mgmt Frame Format

- Used to manage communications between stations and APs
  - Such as management of associations
  - Requests, response, reassociation, dissociation, and authentication

MAC Management

- Synchronization: finding and staying with a WLAN- synchronization functions
- Power Management: sleeping without missing any messages, power management functions
- Roaming: functions for joining a network- changing access points, scanning for access points
- Scanning

Power Management

- Mobile devices are battery powered
  - Power management is important for mobility
- 802.11 power management protocol
  - Allows transceiver to be off as much as possible
  - Transparent to existing protocols
- Allow idle stations to go to sleep
  - Station’s power save mode stored in AP
- APs buffer packets for sleeping stations
  - AP announces which stations have frames buffered
  - Traffic indication map (TIM) sent with every beacon
- Power saving stations wake up periodically

Roaming

- Mobile stations may move:
    - Beyond the coverage area of their AP
    - But within range of another AP
- Re-association allows station to continue operation

Roaming Methodology

- If station decides that link to its current AP is poor:
    - Station uses scanning function to find another AP
    - Station sends re-association request to new AP
- If re-association response is successful:
    - Then station has roamed to the new AP
    - Else station scans for another AP
- If AP accepts re-association request:
    - AP indicates re-association to the distributed system
    - Distributed system information is updated

Scanning

- Scanning required for many functions:
  - Finding and join a network
  - Finding a new access point during roaming
- Passive scanning: Finding networks by listening for beacons
- Active scanning: Each channel sends a probe and waits for probe response

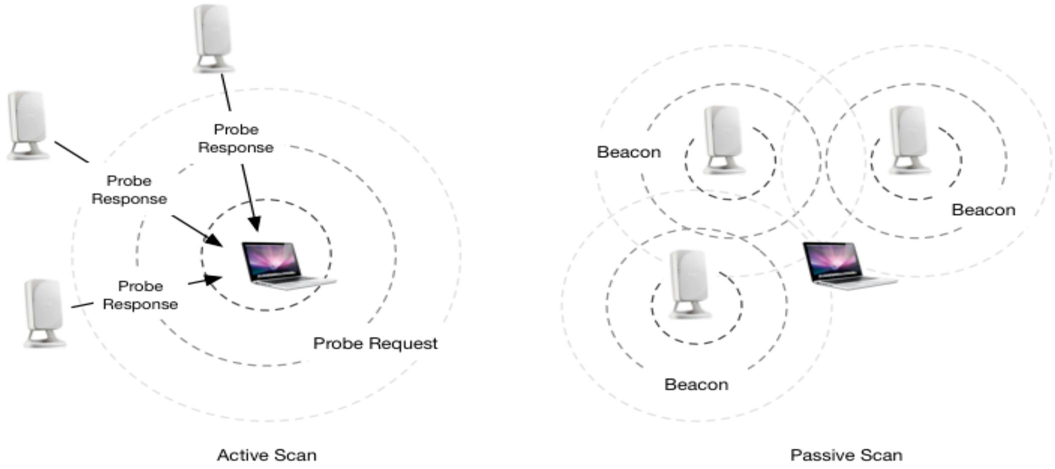


Figure xx: title

Source: Adrian (2017). Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Synchronization

- Timing synchronization function (TSF)
- Used for power management
  - Beacons sent at well-known intervals
  - All station timers in BSS are synchronized

Small Group Discussion

- Research common capabilities of the 802.11 MAC:
    - Understanding the architecture and operating of ad-hoc
    - Infrastructure networks by examining phases of station authentication and association
    - Understanding the operation and behavior of IEEE 802.1X authentication

Wifi Connection – Architectures

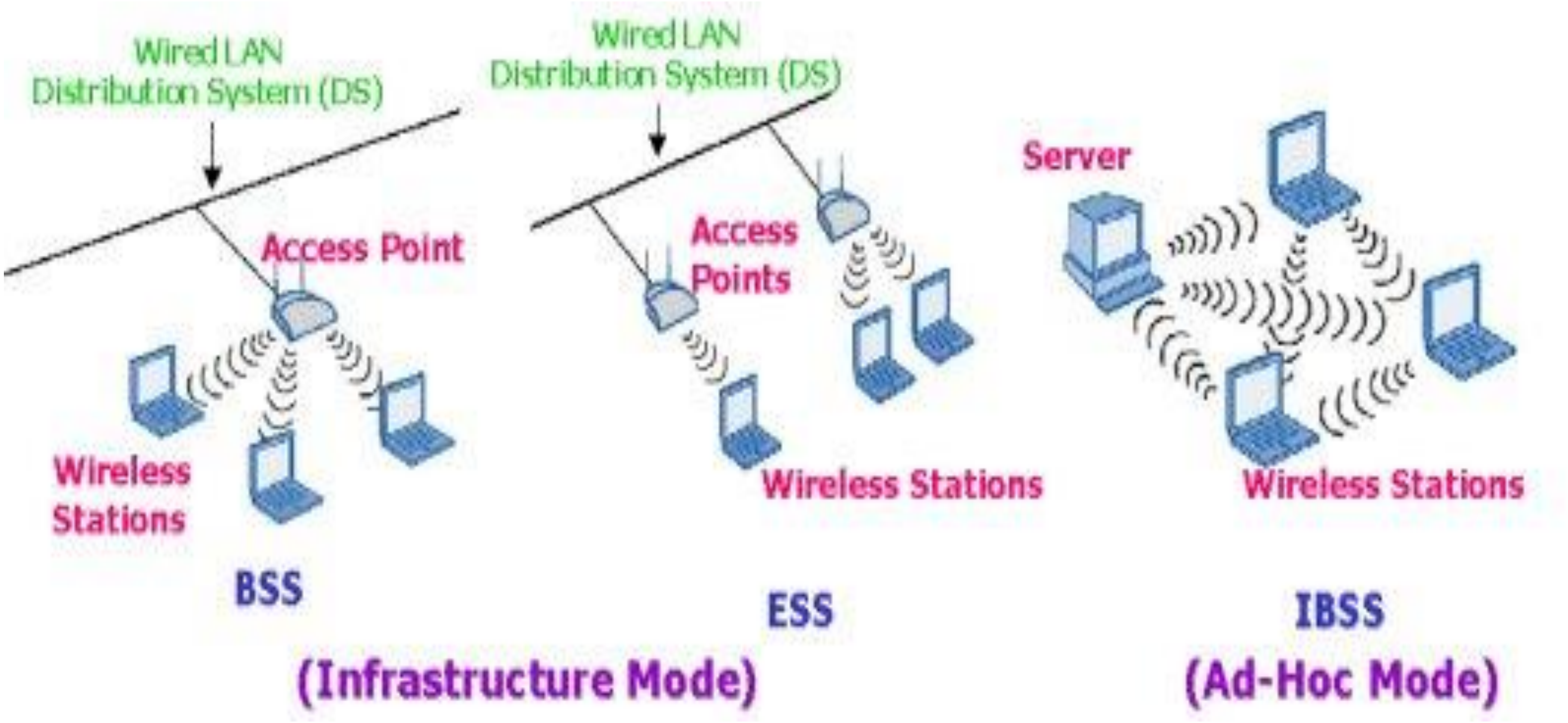


Figure xx: title

Source: Suresh, S. (2011). Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

WiFi Connection: Auth/Association

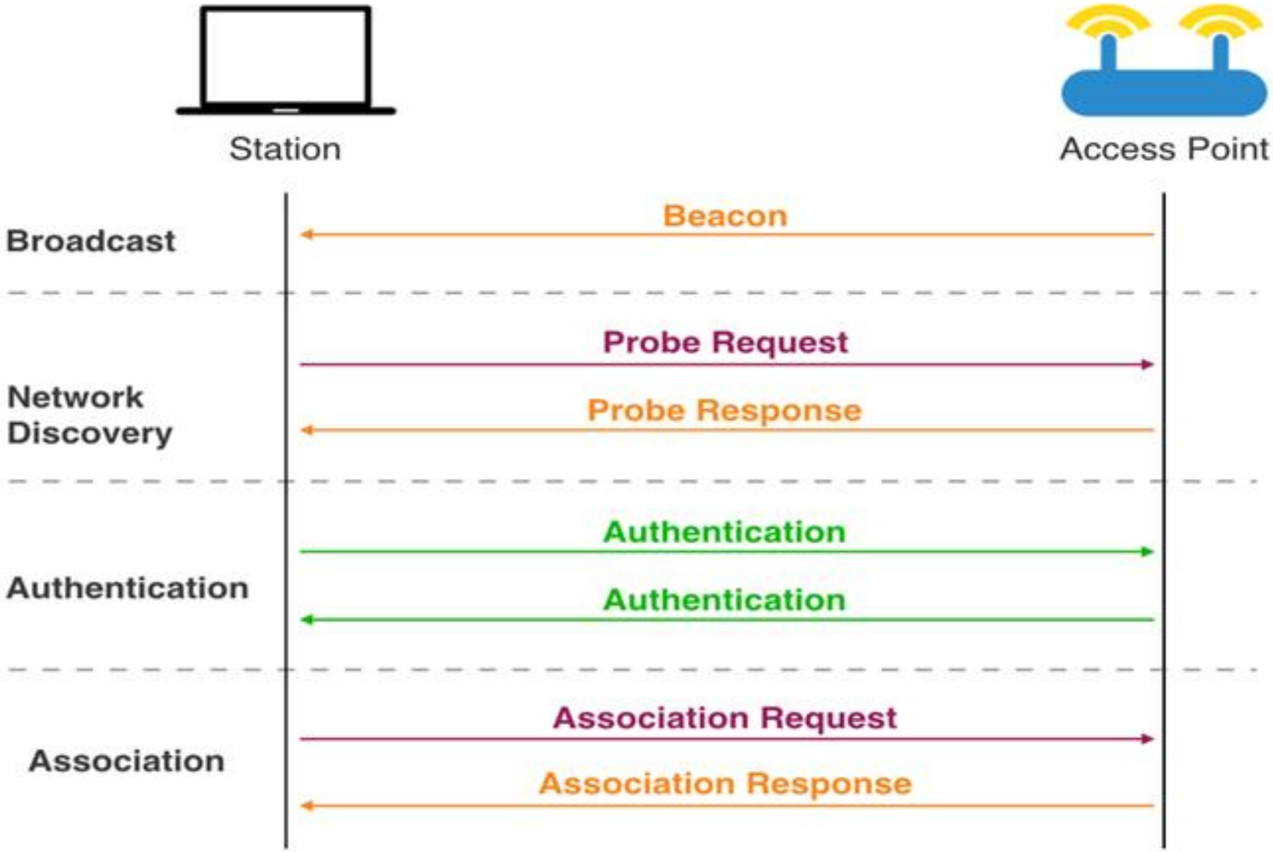


Figure xx: Title

Source: Vergès, F. (2017). Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

802.11 802.1X Authentication

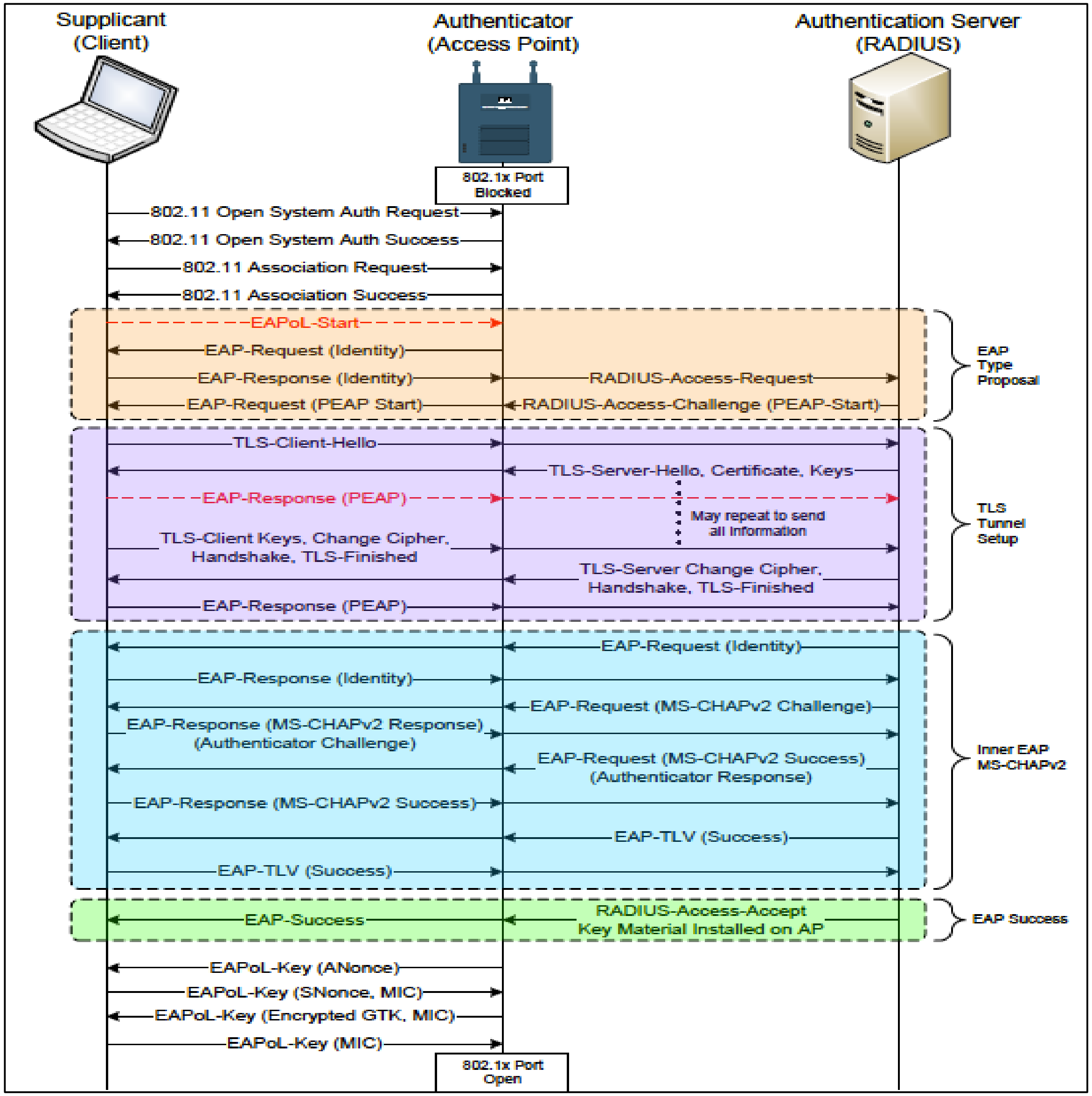

Supplicant (Client)
Authenticator (Access Point)
Authentication Server (RADIUS)
802.1x Port Blocked
802.11 Open System Auth Request
802.11 Open System Auth Success
802.11 Association Request
802.11 Association Success
EAPoL-Start
EAP-Request (Identity)
EAP-Response (Identity)
RADIUS-Access-Request
EAP-Request (PEAP Start)
RADIUS-Access-Challenge (PEAP-Start)
EAP Type Proposal
TLS-Client-Hello
TLS-Server-Hello, Certificate, Keys
EAP-Response (PEAP)
May repeat to send all information
TLS-Client Keys, Change Cipher, Handshake, TLS-Finished
TLS-Server Change Cipher, Handshake, TLS-Finished
EAP-Response (PEAP)
TLS Tunnel Setup
EAP-Request (Identity)
EAP-Response (Identity)
EAP-Request (MS-CHAPv2 Challenge)
EAP-Response (MS-CHAPv2 Response) (Authenticator Challenge)
EAP-Request (MS-CHAPv2 Success) (Authenticator Response)
EAP-Response (MS-CHAPv2 Success)
EAP-TLV (Success)
EAP-TLV (Success)
Inner EAP MS-CHAPv2
EAP-Success
RADIUS-Access-Accept Key Material Installed on AP
EAP Success
EAPoL-Key (ANonce)
EAPoL-Key (SNonce, MIC)
EAPoL-Key (Encrypted GTK, MIC)
EAPoL-Key (MIC)
802.1x Port Open

Figure xx: Title
Source: VonNagy, A., 2012. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

References

Adrian (2017). Understanding the Scan Modes in WiFi Explorer Pro. Retrieved from https://www.adriangranados.com/blog/understanding-scan-modes-wifiexplorerpro

Goliya, A. (2003). Dynamic Adaption of DCF and PCF mode of IEEE 802.11 WLAN. Retrieved from https://www.slideserve.com/ethel/dynamic-adaption-of-dcf-and-pcf-mode-of-ieee-802-11-wlan

Habbani, N. F. I. (2004). Investigations of a Multi-Cell Wireless LAN Under Different Load Distributions. University of Khartoum. Retrieved from http://khartoumspace.uofk.edu/bitstream/handle/123456789/9898/Investigations%20of%20a%20Multi-Cell%20Wireless%20LAN.pdf?sequence=1&isAllowed=y

Hada, R. (2013). WLAN – IEEE 802.11. Retrieved from https://www.slideshare.net/rahulhada/wlan-ieee-80211

References

Hong, C. S. (2004). Introduction to Wireless LAN. Retireved from http://networking.khu.ac.kr/html/lecture_data/Advance_Internet_Protocol/Wireless%20LAN%20(May%202004).pdf

Nayanajith, R. (2014). CWAP – 802.11 Fragmentation. Retrieved from https://mrncciew.com/2014/11/03/cwap-802-11-fragmentation/

Netprojnetworks (2017). Retrieved from http://www.netprojnetworks.com/frame-changes-802-11n/

Sarker, M. (2017) Development of a CSMA MAC protocol and throughput analysis for MU-MIMO WLAN. Bangladesh University of Engineering. Retrieved from https://www.researchgate.net/publication/319206105_development_of_a_csma_mac_protocol_and_throughput_analysis_for_mu-mimo_wlan

Suresh, S. (2011). IEEE 802.11. Retrieved from https://www.slideshare.net/subbiahsuresh/ieee-80211-8822887

References

Vergès, F. (2017). How to check if a client device supports 802.11v. Retrieved from https://www.semfionetworks.com/blog/how-to-check-if-a-client-device-supports-80211v

VonNagy, A. (2012). Is WPA2 Security Broken Due to Defcon MS-CHAPv2 Cracking? Retrieved from http://revolutionwifi.blogspot.com/2012/07/is-wpa2-security-broken-due-to-defcon.html

For more information, contact:
Director, Centre for Instructional Technology and Development
Southern Alberta Institute of Technology
1301 16 Ave. N.W., Calgary, AB T2M 0L4