Answers for Session 3d - Data Transfer and Aggregation

1. In the TXOP case, If the sender keeps on sending the data receiver without checking contention medium 2nd time What about remaining devices which are in queue to send/receive data ??

In a TXOP (Transmission Opportunity) case, a sender can continuously transmit data to a receiver without checking for contention on the medium for a specific time. For Every txOP there is a time limit. So that other devices are not starving. After the time specified to that client is finished

2. How to add data rate and Payload column in wireshark

You can add any parameter into the column by selecting the field, right clicking and selecting as apply column.

To add the payload. In QoS data frames got to

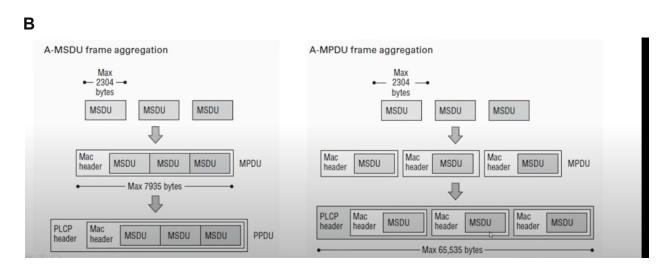
Go to -> QoS control -> Payload type

🔳 🖉 💿 🚞 🔁 💆	3 ९ ⇔ ⇔ ≅ 7 ₺ 📜 🗏 ९ ९ ९ ୩			
wlan.fc.type_subtype==40				
Destination	Info	Protocol Length Tag Number	Frame 22149: 1404 bytes on wire (11232 bits), 1404 bytes capt	ured (11232 bits) on interface
5a	QoS Data, SN=3737, FN=0, Flags=.pF.	802.11 432	> Radiotap Header v0, Length 76	
e:c1:b	QoS Data, SN=1355, FN=0, Flags=.pRT	802.11 1404	> 802.11 radio information	
:c1:b	QoS Data, SN=1356, FN=0, Flags=.pT	802.11 1404	V IEEE 802.11 QoS Data, Flags: .pT	
:c1:b	QoS Data, SN=1357, FN=0, Flags=.pT	802.11 1404	Type/Subtype: QoS Data (0x0028)	
:c1:b	QoS Data, SN=1358, FN=0, Flags=.pT	802.11 1404	> Frame Control Field: 0x8841	
:c1:b	QoS Data, SN=1359, FN=0, Flags=.pT	802.11 1404	.000 0000 0011 1000 = Duration: 56 microseconds	
:c1:b	QoS Data, SN=1360, FN=0, Flags=.pT	802.11 1404	Receiver address:	
:c1:b	QoS Data, SN=1361, FN=0, Flags=.pT	802.11 1404	Transmitter addre	
:c1:b	QoS Data, SN=1362, FN=0, Flags=.pT	802.11 1404	Destination addre	
:c1:b	QoS Data, SN=1363, FN=0, Flags=.pT	802.11 1404	Source address: I	
:c1:b	QoS Data, SN=1364, FN=0, Flags=.pT	802.11 1404	BSS Id: Cisco_5f:	
:5a	QoS Data, SN=2069, FN=0, Flags=.pF.	802.11 150	STA address: Inte	
:5a	QoS Data, SN=2478, FN=0, Flags=.pF.	802.11 150	0000 = Fragment number: 0	
:c1:b	QoS Data, SN=2936, FN=0, Flags=.pRT	802.11 1404	0101 0101 0010 = Sequence number: 1362	
c1:b	QoS Data, SN=2937, FN=0, Flags=.pT	802.11 1404	V Qos Control: 0x4210	
c1:b	QoS Data, SN=2938, FN=0, Flags=.pT	802.11 1404	00000 = TID: 0	
c1:b	QoS Data, SN=2939, FN=0, Flags=.pT	802.11 1404	[000 = Priority: Best Effort (Best Effort	t) (0)]
:c1:b	QoS Data, SN=2940, FN=0, Flags=.pT	802.11 1404	= QoS bit 4: Bits 8-15 of QoS Control	1 field are Queue Size
:c1:b	QoS Data, SN=2941, FN=0, Flags=.pT	802.11 1404	00 = Ack Policy: Normal Ack (0x0)	
:c1:b	QoS Data, SN=2942, FN=0, Flags=.pT	802.11 1404	0 = Payload Type: MSDU	
c1:b	QoS Data, SN=2943, FN=0, Flags=.pT	802.11 1404		Expand Subtrees
c1:b	QoS Data, SN=2944, FN=0, Flags=.pT	802.11 1404		Collapse Subtrees
c1:b	QoS Data, SN=2945, FN=0, Flags=.pT	802.11 1404		Expand All
Sa	QoS Data, SN=2870, FN=0, Flags=.pF.	802.11 150		Collapse All
c1:b	QoS Data, SN=438, FN=0, Flags=.pT	802.11 1404	1	Apply as Column Ctrl+Shit
c1:b	QoS Data, SN=439, FN=0, Flags=.pT	802.11 1404		
c1:b	QoS Data, SN=440, FN=0, Flags=.pT	802.11 1404		Apply as Filter
c1:b	QoS Data, SN=441, FN=0, Flags=.pT	802.11 1404	P	Prepare as Filter
c1:b	QoS Data, SN=442, FN=0, Flags=.pT	802.11 1404		Conversation Filter
c1:b	QoS Data, SN=443, FN=0, Flags=.pT	802.11 1404	(Colorize with Filter
c1:b	QoS Data, SN=444, FN=0, Flags=.pT	802.11 1404	F	Follow
c1:b	QoS Data, SN=445, FN=0, Flags=.pT	802.11 1404		Сору
c1:b	QoS Data, SN=446, FN=0, Flags=.pT	802.11 1404		odbi.
c1:b	QoS Data, SN=447, FN=0, Flags=.pT	802.11 1404	2	Show Packet Bytes Ctrl+Shit
Sa	QoS Data, SN=3271, FN=0, Flags=.pF.	802.11 150	5	Export Packet Bytes Ctrl+Shit
c1:b	QoS Data, SN=2024, FN=0, Flags=.pT	802.11 1404		
c1:b	QoS Data, SN=2025, FN=0, Flags=.pT	802.11 1404		Wiki Protocol Page
c1:b	QoS Data, SN=2026, FN=0, Flags=.pT	802.11 1404		Filter Field Reference
c1:b	QoS Data, SN=2027, FN=0, Flags=.pT	802.11 1404	P	Protocol Preferences
1:b	QoS Data, SN=2028, FN=0, Flags=.pT	802.11 1404	1	Decode As Ctrl+Shit
c1:b	OoS Data, SN=2029, FN=0, Flags=.pT	802.11 1404		Go to Linked Packet
:c1:b	OoS Data, SN=2030, FN=0, Flags=.pT	802.11 1404		Show Linked Packet in New Window
c1:b	OoS Data, SN=2031, FN=0, Flags=.pT	802.11 1404		

To add the data rate of any packet Go to -> 802.11 radio information -> Data rate

Apply a displ	ay filter <ctrl-></ctrl->						
	Destination	Info	Protocol Length Tag Number	> Frame 2: 97 bytes on wire (776	i bits), 97 bytes captu	ured (776	bits)
lc:		Beacon frame, SN=4006, FN=0, Flags=	802 468 SSID parameter set, Sup	Radiotap Header v0, Length 48			
dc:		FILS Discovery, BI=100	802 97 Tx Power Envelope	Header revision: 0			
58:		Probe Request, SN=229, FN=0, Flags=	802 183 SSID parameter set,Sup	Header pad: 0			
dc:		Probe Response, SN=7, FN=0, Flags=	802 462 SSID parameter set,Sup	Header length: 48			
dc:		FILS Discovery, BI=100	802 97 Tx Power Envelope	> Present flags			
b8:		Probe Request, SN=230, FN=0, Flags=	802 190 SSID parameter set,Sup	MAC timestamp: 77609278			
dc:		Probe Response, SN=8, FN=0, Flags=	802 462 SSID parameter set,Sup	> Flags: 0x00			
dc:		FILS Discovery, BI=100	802 97 Tx Power Envelope	Data Rate: 6.0 Mb/s			
dc:		FILS Discovery, BI=100	802 97 Tx Power Envelope	Channel frequency: 5975 [A	Expand Subtrees		
dc:		Beacon frame, SN=4011, FN=0, Flags=	802 468 SSID parameter set,Sup	> Channel flags: 0x0140, Ort	Collapse Subtrees Expand All		lexing (OFDM), 5 GHz
dc:		FILS Discovery, BI=100	802 97 Tx Power Envelope	Antenna signal: -69 dBm	Collapse All		
b8:		Authentication, SN=231, FN=0, Flags=	802 90 Vendor Specific	Antenna noise: -98 dBm			
		Acknowledgement, Flags=	802 58	Antenna: 0	Apply as Column	Ctrl+Shift+I	
dc:		Authentication, SN=0, FN=0, Flags=	802 78	> Vendor namespace: AtherosC	Apply as Filter	•	
		Acknowledgement, Flags=	802 58	> 802.11 radio information	Prepare as Filter	•	
b8:		Association Request, SN=232, FN=0, Flags=	802 285 SSID parameter set,Sup	> IEEE 802.11 Action, Flags: .	Conversation Filter		
		Acknowledgement, Flags=	802 58	> IEEE 802.11 Wireless Managem	Colorize with Filter Follow		
b8:		Data, SN=0, FN=0, Flags=.pF.	802 96				
dc:		FILS Discovery, BI=100	802 97 Tx Power Envelope		Сору	•	
dc:		Association Response, SN=0, FN=0, Flags=	802 349 Supported Rates, RM Ena		Show Packet Bytes	Ctrl+Shift+O	
		Acknowledgement, Flags=	802 58		Export Packet Bytes	Ctrl+Shift+X	
dc:		FILS Discovery, BI=100	802 97 Tx Power Envelope		Wiki Protocol Page		
dc:		Key (Message 1 of 4)	EAPOL 181		Filter Field Reference		
		Acknowledgement, Flags=	802 58		Protocol Preferences	•	
dc:		Beacon frame, SN=4016, FN=0, Flags=	802 402 SSID parameter set, Sup		Decode As	Ctrl+Shift+U	
dc:		FILS Discovery, BI=100	802 97 Tx Power Envelope		Go to Linked Packet		
8:		Key (Message 2 of 4)	EAPOL 209 RSN Information		Show Linked Packet in New Window		
		Acknowledgement, Flags=	802 58				
dc:		Key (Message 3 of 4)	EAPOL 269				
		Acknowledgement, Flags=	802 58				
ic:		FILS Discovery, BI=100	802 97 Tx Power Envelope				
		Key (Message 4 of 4)	EAPOL 181				
		Acknowledgement, Flags=	802 58				
		Acknowledgement, Flags=	802				

3. In A-Mpdu all the msdu's are same or diff and it will go to the same destination ?



Yes, A-MPDU frames can have different destination addresses. This is because each MSDU in an A-MPDU frame has its own MAC trailer, which contains the destination address.

This allows A-MPDU frames to be used to transmit data to multiple destinations simultaneously. For example, a wireless access point could use an A-MPDU frame to transmit data to multiple client devices.

A-MSDU frames, on the other hand, cannot have different destination addresses. This is because A-MSDU frames have a single MAC header, which contains the destination address.

All the aggregated MPDUs must have the same 802.11 receiver address (RA) but can have different MAC-layer destination addresses (DA).

5. For AMPDU frames how the NAV timer will be calculated , I do see aggregated frames NAV timer shows as 0

The NAV timer for AMPDU frames is calculated in the same way as the NAV timer for single-frame transmissions. The NAV timer is calculated as follows:

NAV timer = SIFS + preamble duration + frame duration + DIFS

where:

- SIFS is the Short Interframe Space, which is a 16 microsecond delay.
- preamble duration is the duration of the preamble, which is 12 microseconds for 802.11n and 20 microseconds for 802.11ax.
- frame duration is the duration of the frame, which is calculated as follows:

frame duration = PHY header duration + MPDU duration + PHY trailer duration where:

- PHY header duration is the duration of the PHY header, which is 20 microseconds for 802.11n and 24 microseconds for 802.11ax.
- MPDU duration is the duration of the MPDU, which is calculated as follows:

MPDU duration = data rate * MPDU length / 8

where:

- data rate is the data rate of the transmission in bits per second.
- MPDU length is the length of the MPDU in bytes.
- PHY trailer duration is the duration of the PHY trailer, which is 4 microseconds for 802.11n and 6 microseconds for 802.11ax.

Once the NAV timer has been calculated, it is included in the preamble of the AMPDU frame. All other devices in the vicinity will listen for the NAV timer and will not transmit until the NAV timer expires.

6.Why do aggregated frames show NAV timer as 0?

There are a few reasons why aggregated frames NAV timer may show as 0:

- The device may not be calculating the NAV timer correctly.
- The device may be using a newer version of the 802.11 standard that does not require the NAV timer to be included in the preamble of aggregated frames.
- The device may be using a proprietary protocol that does not require the NAV timer to be included in the preamble of aggregated frames.