NET3900: Midterm Review

A: Wi-Fi Basics

Q1/2. A certain ESS has 15 dual-radio Aruba Access Points. The Access Points are each configured with 3 SSIDs in the 2.4 GHz band and 4 SSIDs in the 5 GHz band. How many unique BSSIDs are there in this ESS? Show calculations to support your answer.

- 15 APs x (3 + 4) SSIDs = 105

B: Modulation

Q3/4. Calculate the PHY rate for a Wi-Fi, 802.11ac radio with the following specs:

- Amplitude Modulation levels per QAM carrier: 16
- Number of bonded channels: 4
- Number of data bits for 1 redundancy bit: 5
- Guard Interval to support a maximum delay spread of 80 ns.
- 4 x 4 MIMO

- PHY = NBRS/Tb

AM levels = 16 therefore 256 constellation points → 8 bits per symbol (i.e. $2^8 = 256$)

4 bonded channels → 234 carriers

R= 5/(5+1)

GI = 400 ns

4 MIMO streams = 4 spatial streams

PHY=234x8x(5/6)x4/(3.2 + 0.4) = 1733 Mbps

C: Wi-Fi Protocol

Q4/5. The Distributed Coordination Function (DCF) is the algorithm used to determine when a station can transmit. A Wi-Fi wireless station has a message to transmit, but the channel is currently busy.

a) First, the wireless station waits for a clear channel. What two mechanisms does DCF use to determine that the channel is clear and explain their basic operation?

i) Physical Carrier Sense/Clear Channel Assessment: detects RF energy in the channel

ii) Virtual Carrier Sense/NAV Timer: wait for expiry of NAV timer. NAV timer is included in the frame transmitted by a station.

b) Next, the wireless station must wait until its turn to transmit its message. What two mechanisms does DCF use to determine when it's the station's turn to transmit and explain their basic operation?

i: Interframe Spacing: Used to distinguish message priority. Higher priority messages have shorter IFS.

ii) Contention Window: Random time slot selected by the station from within a time window called the contention window. The station waits for this time slot to arrive before sending its message.

c) How does a station determine that its transmission has failed?
- no ACK after timeout period

d) Following a failed transmission, the Contention Window size is doubled. How does this increase the likelihood that the next transmission attempt will be successful?
- distributes backoff values over larger window reducing likelihood of collision

e) Given two messages with parameters shown in the table, which message # will transmit first? Explain your answer.

#	Data Frame Duration	CCA Duration	Contention Window Backoff-Value	Interframe Spacing	NAV Timer
1	50 us	35 us	20 us	65 us	40 us
2	150 us	35 us	45 us	45 us	25 us

#	CCA/NAV	IFS	CW	TOTAL
1	40	65	20	125
2	35	45	45	125

D: Security

Q5/4. Complete the table by answering the following questions.
a) Identify whether each encryption protocol listed is symmetric or asymmetric.
b) Identify whether each encryption protocol listed is 1-way or 2-way.
c) Identify where each protocol is used in the 802.1X/PEAP authentication process.

Encryption Protocol	**Symmetric or Asymmetric**	**1-way or 2-way cypher**	**Usage**
RSA (Rivest,Shamir, Adleman)	A	B	C
SHA (Secure Hash)	D	E	F
RC4 (Ryvest Cypher 4)	G	H	I
AES (Advanced Encryption Standard)	J	K	L

A=asym B=2w C=signing certs
D=NA E=1w F=hash signatures
G=sym H=2w I=data encrypt
J=sym K=2w L=data encrypt

1/2. Each carrier is modulated using QAM. Briefly explain QAM?

QAM modulates a signal by varying the phase and amplitude. In practice, the same effect is achieved by Amplitude Modulating (AM) two orthogonal carriers (i.e. cos, sin) and summing the result. The number of AM levels is determined by how many bits per symbol are needed.

2/3. Your 802.11n Wi-Fi radio is operating with the following configuration:

- 20 MHz Channel
- Number of subcarriers N = 52
- Number of MIMO spatial stream S = 2
- 16-QAM
- FEC Rate R = ¾
- Guard Interval GI = 800 ns
- Base Symbol Time Ts = 3.2 us

Calculate the PHY rate.

First calculate B; $2^B = 16$, therefore B = 4.

Then calculate the PHY rate.

PHY rate = N x B x R x S / (Ts+GI)

= 52 x 4 x ¾ x 2 / (3.2+0.8)us

= 78 Mbps

3/3. Explain three mechanisms that the AP uses to learn the IP address of its controller.

1. The AP Broadcast/Multicasts a query for a Controller using ADP (Aruba Discovery Protocol)
2. The AP sends a query to DNS with the Controller's FQDN
3. The DHCP reply includes the Controller address as an option 43 parameter

4/5. Answer the following questions regarding tunneling protocols.

a) Explain the basic principle of network tunneling?

b) - tunneling embeds/encapsulates a frame into the data field of another frame/packet which carries the embedded frame across the network.

c) Which devices are the tunnel end-points for the AP in an Aruba wireless topology?

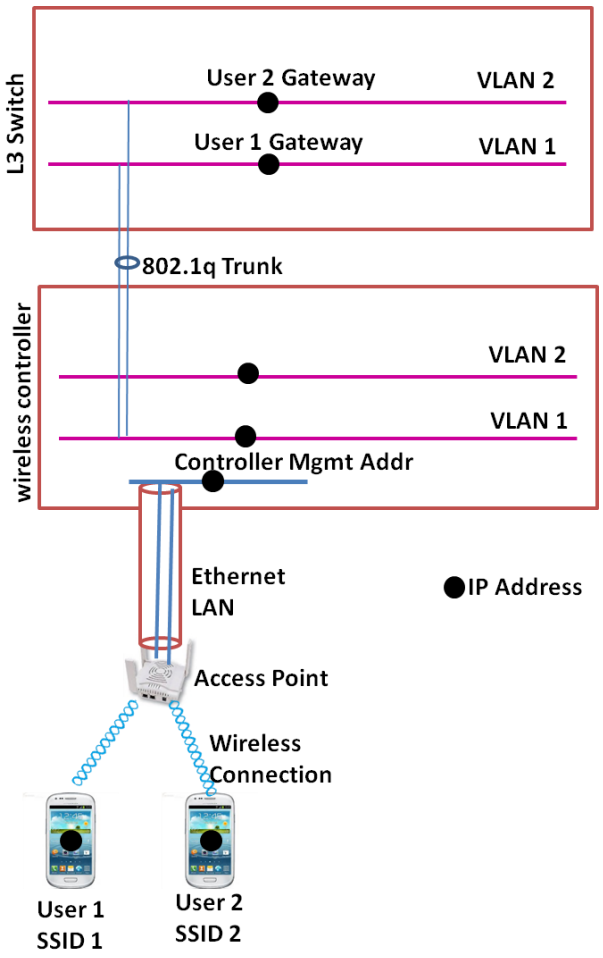
The tunnel end-points for the tunnel are the AP and the Controller (independent of network topology that connects the AP to the controller)

d) Why are they called the tunnel end-points?

- Both the AP and the Wireless Controller encapsulate/de-encapsulate the 802.11 user frame to/from the tunnel.

Q17/2. The following diagram shows an AP connected to a wireless controller via an Ethernet LAN. Two users are associated to two SSIDs. SSID1 connects users to VLAN1 and SSID2 connects users to VLAN2. The users' gateways are configured on the L3 switch. User 1 sends a frame to user 2. Describe, in point form, the path that a frame takes from user 1 until it reaches user 2. Include the following: encryption/decryption points, encapsulation/decapsulation points, Role and Policy decision points, Layer 2 and 3 forwarding points.

- encrypt frame at client
- transmit to AP
- AP encapsulates
- Controller decapsulates
- frame placed on user VLAN1
- frame is translated to 802.3 and switched to gateway address on switch
- frame is routed to destination gateway
- destination device is on this VLAN so gateway ARPs for dest device
- ARP broadcast reaches controller
- Controller answers ARP as ARP proxy device
- Controller switches frame to user VLAN on controller
- controller translates frame back to 802.11
- Controller encapsulates frame and places into GRE tunnel
- Frame received by AP and decapsulated
- frame sent to wireless station over the air
-

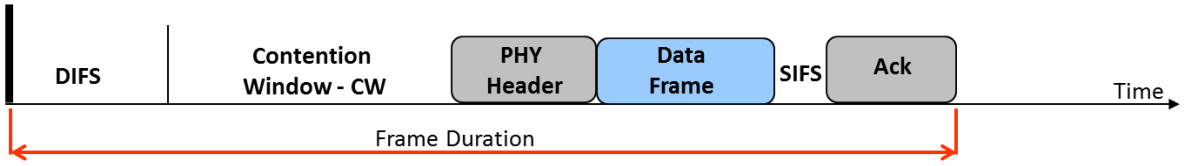


5/2. An AP is connected to VLAN 101. However the wireless client associated to that AP is connected to VLAN 14. How is this accomplished?

This is accomplished using tunneling.

The AP routes its packets to the controller using the outer frame which is connected to VLAN 101. The user frame is carried as the inner frame to the controller. The controller removes the frame and switches it on user VLAN 14.

1/10. The 802.11n standard includes a feature called Frame Aggregation. This means that several data frames are transmitted together during a Wi-Fi transmission.



a) Calculate the Data Throughput for a typical Data Frame size of 100 Bytes. The total overhead (i.e. Frame Duration – Data Frame Duration) is 150 us. The PHY rate is 80 Mbps. Show your detailed calculations. The parameters have been chosen to simplify the arithmetic.

First calculate the Data Frame Duration (DFR)
DFR = (8* 100) bits / 80 Mbps = 10 usec

Throughput = #DataBitsperFrame / TotalFrameDuration
= (8 x 100) bits / (150 + 10) us
= 800 bits / 160 usec
= 5 Mbps

b) Frame Aggregation is now applied and 10 Data Frames are aggregated and transmitted together in one Wi-Fi transmission. The Data Frame size for each of the 10 data frames is still 100 Bytes. One Ack is required for all 10 Data Frames as shown in the diagram. What is the improved Data Throughput Rate.

Throughput = #DataBitsperFrame / TotalFrameDuration
= (8 x 100 x 10) bits / (150 + 10 x 10) us
= 8000 bits / 250 usec
= 32 Mbps

c) What is the purpose of the Contention Window?
The Contention Window helps avoiding transmission collisions. Each station selects a random time from the Contention Window Interval. The station waits this amount of time before attempting to transmit. Since the CW wait time is randomly selected, it reduces that the likelihood that more than one station will transmit at the same time

Q3/8 marks: The DCF algorithm is used to determine which station is allowed to seize the channel next. It includes three functions (1) Listen for a Clear Channel, (2) Wait for My Turn, (3) Transmit.
a) What two methods are used to listen for a clear channel?

- Clear Channel Assessment
- NAV Timer

b) Describe the basic operation of the methods in a).

- measure Wi-Fi RF energy
- timer based on the Duration field

c) What two methods are used for wait for my turn?

- Inter Frame Spacing
- Contention Window

d) Describe the basic operation of the methods in c).

- fixed wait time
- wait time random sample from contention window size

Q4/5 marks: Consider an 802.11ac radio with the following characteristics.

- 80 MHz channel
- FEC rate = 5/6
- MIMO with 6 spatial streams
- 256-QAM
- Guard Interval = 800ns

What is the PHY rate?

- PHY = NBRS/Ts
- N= 234 from table
- B: 256 QAM □ 16 x 16 points □ 4 bits x 4 bits □ 8bits
- Ts: 4 us from table

PHY = 234 x 8 x 5/6 x 6 / 4u = 2.3 Gbps

Q12/12 marks: The following questions refer to controller based architectures.

a) What two types of tunnels are used and explain their purpose.

- Access Tunnel: Tunnels frames between the split MAC layers
- Mobility Tunnel: Carriers VLAN tagged frames from the foreign controller to their home controller

b) Identify and describe three mechanisms that are used by the Access Point to discover the Controller.

- DHCP option codes
- DNS lookup
- broadcast discovery

c) After the Access Point connects to the controller, it sends what two files?

- updated software image
- AP configuration file

f) What is Layer 2 Mobility?

- when a station moves to another controller connected to same VLAN then the IP address of the client does not need to change, this is layer 2 mobility;

g) What is Layer 3 Mobility?

- when a station moves to another controller not connected to same VLAN then the IP address needs to change; this is layer 3 mobility

h) What is the main issue with Layer 3 Mobility and how is it solved?

- requires IP address change but this disrupts various applications such as VoIP or HTTP.
- solution is to tunnel user frames back to home controller so IP address does not need to change

Q13/8 marks: The following questions refer to Wi-Fi security.

a) What two aspects of security are addressed by 802.11 standards?

- user authentication
- data security (i.e. encryption)

b) What three roles/functions are defined by 802.1X. These roles are held by the Wireless Station, Access Point and RADIUS server in the diagram.

- in same order: supplicant, authenticator, authentication server

c) Briefly describe the operation of Part B in the 802.1X/EAP authentication as shown in the diagram.

d) How does Part B differ when using PSK (Pre Shared Keys).

- no need for authentication server
- PSK is used in place of PMK; PSK may be derived from alphanumeric passphrase

Q16/ 5 marks: You are setting up an 802.11n Wi-Fi system in a large conference hall as shown in the diagram. The room is 80 meters long and 40 meters wide. You need to ensure that an Access Point placed at one end of the room can send a signal to a wireless station at the other end of the room without distortion. The Access Point is using an omnidirectional antenna. An object against one wall (see diagram) is causing reflection. Assume that there are no other reflections. An RF signal travels at $3*10^8$ meters/second.

a) What is the value of Delay Spread in nanoseconds?

- Direct Path Delay = distance / c (speed of light)

Direct Path = $80m/3x10^8$ = 267 nanoseconds

Reflected Path = $100/3x10^8$ = 333 nanoseconds

Therefore Delay Spread = 333-267 = 66 nanoseconds

b) What is the minimum Guard Interval that you can use?

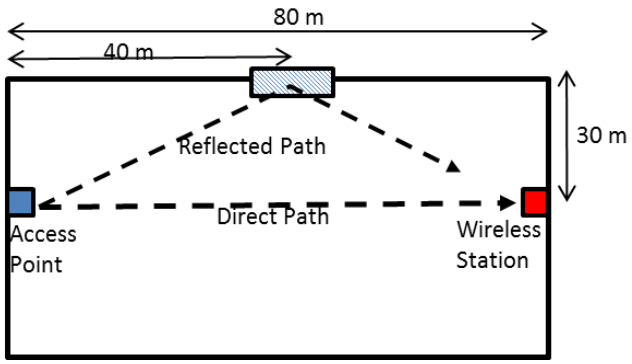
- GI = 400 nanoseconds (min 11n value); also accept 66 nanoseconds

c) What would be the impact of using a Guard Interval which exceeds the calculated minimum?

- reduces capacity

d) What would be the impact of using a Guard Interval which is below the calculated minimum?

- increases Inter Symbol Interference which may lead to increased errors



Q1/1: What is the difference between an access point and a wireless station in terms of standards-based definitions?
- both have an 802.11 compliant protocol stack
- AP also provides access to the distribution system

Q2/1: One un-associated wireless station is in a room with one Access Point. Does this form a basic service set and why?
- no, station must be associated to form an BSS

Q3/1: What is the purpose of the beacon in a BSS?
- provides info to facilitate association, provides synchronization information

Q4/1: Two adjacent APs that can hear each other use the same SSID. Will this cause any interference or confusion to the wireless stations and why?
- no because this is standard use for an ESS, assuming non adjacent channels used

Q5/2: What is the maximum number of non-overlapping channels available in the ISM band as used in Canada? What are they?
3 channels, 1,6,11

Q6/1: At what general frequency do the UNII band and ISM bands operate?
UNII-5GHz; ISM-2.4GHz

Q7/5: The DCF algorithm is used to determine which station is allowed to seize the channel next. The following questions refer to the DCF algorithm.

a) What is the purpose of the contention window and how do stations use the contention window?
- used to separate stations in time
- stations select a random time within the contention window, then station waits this random time before transmitting. The station with the lowest random time transmits first.

b) Two wireless stations are contending for the RF channel. Both stations use a minimum Contention Window of 15 slots (i.e. 135 microseconds). According to the DCF algorithm which station can transmit first?
- station with lowest random contention wait

c) How does a station determine that its frame transmission has suffered a collision?
- no ACK received

d) What adjustments does a station make to the DIFS and Contention Window when retransmitting a frame following a collision?
Increases Contention Window size (doubles) for next transmission unless at max size

e) What are the two mechanisms used by the DCF to determine if the RF channel is available?
- Physical carrier detect using CCA
- Logical carrier detect using NAV timer

Q8/2: 802.3 Ethernet uses 2 MAC addresses whereas Wi-Fi uses four. Why does Wi-Fi use four MAC address and what are their uses.
- four addresses used for source MAC address, destination MAC address, sending radio MAC and receiving radio MAC

Q9/1: Explain the concept of a subcarrier.
- each channel uses multiple carriers called sub carriers which are modulated

Q10/2: Subcarriers are orthogonal. What does this mean and how does OFDM take advantage of this characteristic.
- subcarriers are independent and can be individually modulated without causing interference to other subcarriers despite close frequency spacing

Q11/2: What is a guard interval and why is it used?
- lengthening of the symbol time to protect against signal reflections causing interference (intersymbol interference)

Q12/1: What is the relationship between OFDM and QAM?
- OFDM carriers are modulated using QAM

Q13/2: If I want to encode four bits per symbol using QAM, what size constellation do I need? Explain.
- 4 bits → 2 bits quadrature x 2 bits in-phase → 4 points quadrature x 4 points in-phase → 16 point constellation

Q14/1: What does it mean to have a FEC ratio of 3/4?
- 1 redundancy / error correction bit for every 3 data bits

Q15/2: Your 802.11a Wi-Fi radio tells you that it is operating at a PHY rate of 36 Mbps.

You know that the FEC rate is 3/4 and that the total symbol duration (including guard interval) is 4 microseconds. Calculate the QAM modulation rate in bits per symbol.

PHY rate = NxBxR / Ts

→ 36 Mbps = (48 data carriers x B x ¾) / 4 microseconds

→ B = 4 bits per symbol

Q21/8: Briefly explain the following concepts in terms of purpose and operation:

-channel bonding

> combining channels to double number of carriers per channel, doubles channel bandwidth for higher capacity

- MIMO

> using multiple transmission streams with multiple antennae, also called spatial multiplexing used to increase capacity

- frame aggregation

> sending multiple frames in one Wi-Fi transmission to reduce overhead and increase capacity

- reduced guard interval

> reduce guard interval to reduce total symbol time and therefore increase capacity

Q22/3: Consider an 802.11ac radio with the following characteristics.

- 80 MHz channel
- FEC rate = 5/6
- MIMO with 4 spatial streams
- 256-QAM
- Total Symbol time (including GI) = 4 microseconds

What is the PHY rate?

PHY = NxBxRxS / Tsym

- 80 MHz → 234 subcarriers
- 256-QAM → 16 points x 16 points → 4 bits x 4 bits → 8 bits per symbol

PHY rate = (234 x 8 x 5/6 x 4) / 4 microseconds

PHY rate = 1560 Mbps

Q21/8: Briefly explain the following concepts in terms of purpose and operation:

-channel bonding

> combining channels to double number of carriers per channel, doubles channel bandwidth for higher capacity

- MIMO

> using multiple transmission streams with multiple antennae, also called spatial multiplexing used to increase capacity

- frame aggregation

> sending multiple frames in one Wi-Fi transmission to reduce overhead and increase capacity

- reduced guard interval

> reduce guard interval to reduce total symbol time and therefore increase capacity

Q15. What is the difference between a guard band and a guard interval?

- Guard band is frequency separation used in frequency division multiplexing
- Guard Interval is time separation used to separate the transmission of symbols.
- This separations reduces the chances for intersymbol interference.

Q16. What does it mean when we say that the subcarriers are orthogonal?

- Each subcarrier can be modulated and demodulated independently and without interference from the other subcarriers.