EXAMPLE QUESTIONS

Wi-Fi

1. Describe the MAC used in the DCF function of IEEE 802.11. You should discuss at least the following topics:
    a. Physical carrier sensing and backoff mechanism
    b. Hidden terminal problem
    c. Virtual carrier sensing and RTS/CTS mechanism
    d. Exposed terminal problem

2. Describe the MAC used in the HCF function of IEEE 802.11e. You should discuss at least the following items:
    a. How EDCA access works
    b. How HCCA access works
    c. How the power saving mechanism (U-APSD) works and what are the differences compared to the traditional power saving strategy of 802.11

3. Describe in details the passive and active scanning procedures.
    a. What is their purpose?
    b. What message exchanges are involved in the processes?
    c. Briefly explain at least one advanced service that can be enabled by sniffing active or passive scanning messages with an interface set in monitor mode.

4. Describe in details the process through which a station connects to an access point. What are the messages exchanged in the process?

5. Describe in details how the power save mechanism of 802.11 works. Focus on:
    a. The power management flag in frames transmitted by stations and the Listen Interval
    b. The Traffic Indication Map (TIM) and the Delivery Traffic Indication Message (DTIM)
    c. How an attacker can exploit the power management process to perform a Denial of Service attack against a station

6. Describe how to perform localization exploiting beacons received by in-range access points.
    a. What approach can be used if the locations of the access points are known?
    b. What if the location of the access points are unknown?

7. Describe flooding attacks in WLANs
    a. What is their target? Why are flooding attacks effective?
    b. What messages are generally flooded?

8. Describe at least 2 attacks that can be performed against 802.11 stations and possible countermeasures

Bluetooth

1. Briefly describe the Bluetooth protocol:
    a. Device classes and roles. How is a piconet formed?
    b. Types of connections and corresponding application scenarios

2. Describe the different low power modes of Bluetooth and what effect each node has on the device address.

3. Describe the FHSS transmission method utilized in Bluetooth.

4. Explain how a Bluetooth piconet composed by m nodes (1 master and m-1 slaves) can be modeled as a polling system.
    a. What assumptions should be imposed in order to derive the model?
    b. How many queues are present in the system?
    c. What is the cycle length? What about the token passing time h?

MAC modeling

1. Explain the differences between Scheduled access and Random Access. Provide examples of protocols for the two cases.

2. Explain the differences between exhaustive, gated and limited polling. Consider an exhaustive polling system, with M stations and token passing time h, compute the average time due to passing the token among stations W_3

3. Derive the expected waiting E[W] for a system with exhaustive polling with M stations, frame transmission time T, token passing time h and global rate λ

4. An exhaustive polling system has average waiting time for packets equal to E[W]. In case the same system becomes gated:
    a. Will E[W] increase or decrease? Why? How much?

5. Explain the differences between Pure Aloha and Slotted Aloha. For each case derive the throughput S as a function of the offered traffic G. Such relations are fixed or time-variant?

IP Mobile

1. Provide at least one example of mobility management at:
    a. The MAC layer
    b. The Network layer
    c. The Application layer

2. Explain why the approach used by 802.11 Access Points to manage station mobility at the MAC layer cannot be used at the network layer

3. Explain the basics mechanisms of Mobile IP, focusing in particular on:
    a. Permanent IP address and Home Agent
    b. Care-of-address
    c. Tables needed for registration

4. Explain the problem of ingress filtering and why it affects Mobile IP.

TCP over wireless

1. Explain the issues of applying TCP over wireless channels and the different approaches available to cope with them.

2. Explain the difference between long-lived and short lived connections in TCP. What is the effect of a loss in the two cases?

3. Derive the model for the throughput in long-lived TCP connections assuming one ACK per MSS is transmitted by the receiver and the channel has loss rate equal to p

4. Derive the model for the transfer time of short-lived TCP connection in case of no channel losses.

Ad-Hoc Networks

1. Describe what Ad-Hoc Networks are, their application scenarios and why are different from traditional networks

2. Describe the differences between reactive and proactive protocols. What are their pros and cons?

3. Describe the flooding protocol. Does flooding ensure that the packet is received by the destination?

4. Describe the DSR protocol in case links are asymmetric.

5. Describe the AODV protocol and how it improves over DSR.