1. **(20 points) Voice transmission in wireless systems.**
   a. **What are the main problems when transmitting data using wireless system that were made for voice transmission?**
   Answer:
   Systems optimized for voice transmission support certain fixed data rates and operate circuit switched (4 point). Data transmission happens quite often spontaneous with varying data rates (4 point). Thus either too much bandwidth is reserved to accommodate the maximum expected data rate or data transmission experiences long delays due to connection setup.
   b. **What are the possible steps to mitigate the problems and to raise efficiency?**
   Answer:
   One possible step towards the support of data transmission is the introduction of packet switched services (6 point) as known from the internet. An example is GPRS in GSM.
   c. **How can this be supported by billing?**
   Answer:
   Instead of time-based billing providers can now bill based on volume (6 point) (However, application based billing would make even more sense as customers are not interested in bytes but useful applications)

2. **(15 points) GPRS and HSCSD.**
   a. **Why is a new infrastructure needed for GPRS, but not for HSCSD?**
   Answer:
   HSCSD still operates circuit switched as CSD does. It “simply” combines several connections. GPRS introduces a new paradigm in GSM, packet switching. (6 point)
   b. **Which components are new and what is their purpose?**
   Answer:
   The core network needs routers handling the packet stream (3 point). These routers(SGSN, GGSN) operate on IP and rely on the traditional GSM network for user localization.
   Another new component located at the HLR is a registry for subscribed GPRS services (3 point).
   Furthermore, the system has to set up a context for each active user, account transmitted data, assign IP addresses etc. (3 point)

3. **(10 points) Near-far effect.**
   a. **How does UTRA-FDD counteract the near-far effect?**
   Answer:
   The terminals have to measure and adapt their transmission power (2 point) 1500 times per second (2 point) in UTRA/FDD to achieve equal signal strength (2 point) at the base station.
   b. **Why is this not a problem in GSM?**
   Answer:
   In GSM, this is no problem as it never happens that two stations send at the same time on the same frequency (4 point)

4. **(20 points) Mobility in WLANs. In your answer, think of the capabilities of layer 2 where WLANs reside.**

   a. **How is mobility restricted using WLANs?**

   Answer:

   Without further mechanisms mobility in WLANs is restricted to the coverage of a single access point, authentication of newly roamed mobile users, the need to support of anonymity and privacy for mobile users, etc. (5 point)

   b. **What additional elements are needed for roaming between networks, how and where can WLANs support roaming?**

   Answer:

   In order to support roaming, additional inter access point protocols are needed. (5 point)

   The APs have to inform each other about the current active stations within their coverage. This approach is only feasible for local areas, otherwise location registers etc. similar to GSM required. The APs simply operate as transparent, self-learning bridge that need additional information to " forget" stations faster compared to the aging mechanisms in fixed network bridges. Station identification is based on MAC address. (5 point)

   Roaming typically requires a switched layer-2-network. (5 point)

5. **(20 points) Security issues in WLANs.**

   a. **With a focus on security, what are the problems of WLANs?**

   Answer:

   WLANs introduce the air interface which is very simple to eavesdrop. (8 point)

   b. **What level of security can WLANs (IEEE 802.11 and Bluetooth) provide, what is needed additionally and how far do the standards go?**

   Answer:

   Many WLAN standards introduce more or less strong encryption mechanisms. The most famous one, WEP, has been cracked soon after introduction. Furthermore, the most prominent WLAN family, 802.11, does not provide powerful authentication mechanisms. New standard introduce more security(802.11i), however users should always use an additional VPN on top of the WLAN to protect privacy and data integrity. (6 point)

   WLAN following BLUEtooth or HiperLAN2 offer more advanced security function compared to 802.11. However there are some weakness when it comes to real implementation. The PINs are quite often fixed. Some of the keys are permanently stored on the devices and the quality of the random number generators has not been specified.

   (6 point)

6. **(15 points) How do IEEE 802.11 and Bluetooth, respectively, solve the hidden terminal problem?**

   Answer:

802.11 uses the MACA mechanism sending PTS/CTS (7 point) to solve the hidden terminal problem. For HiperLAN2 this problem doe not exist as the AP controls all medium access. If a terminal is hidden it can not communicate at all and thus, does not interfere. In Bluetooth, too, are no hidden terminals (8 point)as the master controls all visible slaves. If a terminal does not see the master it can not participate in communication. If this terminal sends anyway it will not interfere as this terminal then acts as master with a different hopping sequence.