# A small Test / repetition

Talk and discuss with your neighbour following questions

## The layered communication model (once again just to be sure):

* Describe the 5 layers in the internet model have (the model from the book)
* What is the horizontal communication?
* What is the vertical communication?
* What is a header?
* What is a protocol?

## Application layer:

* What is the purpose of the application layer?
* What is the purpose of the http?
* Which port is http using?
* What is P2P?
* Which types of applications use P2P?
* What is the basic idea behind P2P?
* What are the challenges of the P2P architecture?

## Transport Layer:

* Which types of computers (equipment) is part of the transport layer communication?
* What is UDP an acronym for?
* What is the purpose of UDP?
* Which types of application would prefer UDP as transport protocol?
* The header for the UDP how does it looks like.
* What do the different fields mean?
* What is TCP an acronym for?
* What is the purpose of TCP?
* Which types of application would prefer TCP as transport protocol?
* The header for the TCP how does it looks like.
* What do the different fields mean?
* How does the TCP protocol establish a connection?
* How do the TCP ensure that it deliver a reliable connection?
* How do the TCP handle congestion control?

## Network Layer:

* What are the important network-layer function(s) in datagram network?
* Explain forwarding.
* What is the content of a forward table? Moreover, how to use a forward table?
* What is the fundamental difference between a router and a packet switch (link-layer switch)?
* Take a closer look at fig.4.16 (p.358) and explain the meaning and use of  
  Version, Time to live, Header Length, Datagram Length, Upper-Layer Protocol
* How many bits are in an IPv4 address?
* What is a subnet?
* How can you find the net-id from a network address?
* How many hosts can you approx. have on a class B network?
* Two organisation are given the address space 233.1.1.0/24 respectively 223.1.1.0/16  
  what are the network-ID and the broadcast address in the two net?
* How many devices can get an individual IP-address in the two organisations?
* It is stated, that the world is running out of IPv4-addresses. Why?  
  How to solve this problem?
* What is a NAT-router?
* How many computers/devices can be behind one NAT-router?
* Describe the two ways a Host (Computer) can obtain an IP-address.
* Why do we not just all switch to IPv6?

# Security -- concepts:

* What are the four different goals for security?
* What does each (sub) goal mean?
* For symmetric encryption / decryption, how many key(s) do you have?
* Which goal does symmetric key(s) fulfil?
* For symmetric keys what are the typical length of a key?
* For symmetric keys, name at least two algorithms.
* What are the major problem using symmetric keys
* For asymmetric encryption / decryption, how many key(s) do you have?
* Which goal do asymmetric keys fulfil?
* For asymmetric keys what are the typical length of a key?
* For asymmetric keys, name at least one algorithm.
* What are the major problem using asymmetric keys?
* What is message digest? In addition, a digital signature?
* What is PGP? In addition, how does it make use of encryption/decryption?
* What is SSL? In addition, how does it make use of encryption/decryption?
* When do you use PGP? and SSL?
* Describe the most important C#-classes in a **client** for SSL programming.
* Describe the most important C#-classes in a **server** for SSL programming