Internetworking/Internetteknik, Examination 2G1305
Date: October 19th 2004 at 14:00 – 18:00

KTH/IMIT/LCN

- ***No help material is allowed - You are not allowed to use dictionaries, books, or calculators!***
- *You may answer questions in English or Swedish.*
- *Students from 2G1507 may also make the exam: but please note this specially on the exam if you are such a student.*
- *Please answer each question on a separate page.*
- *Fill in the table on page 2 for each question you have addressed.*
- *The grading of the exam will be completed no later than November 9 2004.*
- *After grading, the exams will be available for inspection at STEX (Q-building).*
- *Deadline for written complaints is November 23 2004.*
- *Course responsible is Olof Hagsand, phone 08-790 42 61.*

Your name:……

Your social security number (personnummer): ……

Your major (utbildningslinje):……..

Total Points: …….	Grade: ……...

Question	Answered	Potential points	Received points
1		5	
2		5	
3		5	
4		5	
5		5	
6		5	
7		5	
8		5	
9		5	
10		5	
11		5	
12		5	

Total	60	

1. General (5p)

The OSI reference model tries to abstract communication into separate layers. The TCP/IP protocol stack is more practical and is based on the original implementation of the protocol stack. The two models are usually used interchangeably, and often map nicely to each other.

a) How do the OSI and TCP/IP layers map to each other? (2p)

b) Following the OSI reference model (and the terminology used in the course), where would you place each of the following communication devices: Bridge, Router, Repeater, Gateway? (2p)

c) Which TCP/IP layer handles naming of nodes? (1p)

2. IP routing versus bridging (5p)

Layer 2 bridging is a popular way to build networks. But using IP routing is seen as a more scalable networking technology, in the sense that it can handle a larger number of nodes and handle more aggregated traffic. Why is this the case? Specifically, you should cover the difference in addressing and forwarding, and how this leads to better scaling in terms of nodes and traffic. (5p)

3. IP Addressing (5p)

a) A diskless client requesting an IP address sends an IP packet to the limited broadcast address. What are the source and destination IP addresses of this packet? (1p)

b) A router is connected to the 202.33.44.128/25 subnet, using the address 202.33.44.129. It sends a multicast packets destined to all hosts on this network. What are the source and destination IP addresses of the packet? (1p)

c) What is the subnet mask of 202.33.44.128/25? (1p)

d) A site creates an IP subnet of a block of classless addresses: 140.34.23.0/27. What is the network address of the subnet? What is the directed broadcast address of the subnet? (1p)

e) Which interval of unicast addresses can be used by hosts and routers on this subnet? (1p)

4. IPv4 fragmentation (5p)

An application sends a message which is 2400 bytes long. It sends the data as one UDP datagram. The message is then transferred from a sender to a receiver over three hops. The first link has an MTU of 1500, the second has an MTU of 1000 bytes, and the third has an MTU of 1200 bytes.

Assume that no PATH MTU discovery and that the IP header is 20 bytes (without options), and a UDP header is 8 bytes. MTU on a link means Max Transmission Unit and is the max *payload* of the link-level frame. The four fragmentation fields in the IPv4 header are: identification, don't-fragment flag (DF), more fragment flag (MF) and fragmentation offset

a) How many fragments will arrive to the IP module at the receiving host and how large will each IP fragment be (headers included)? (3p)

b) What will be the fragmentation field values of each fragment when they have arrived at the receiver? (2p)

5. TCP (5p)

a) There is something called the "silly window" syndrome in TCP. Describe what this is and why it is a problem. (1p)

b) There are two variants of the silly window syndrome. What are the two causes for the silly window syndrome? (1p)

c) Name and explain two ways to solve the silly window syndromes (one for each variant). (3p)

6. Dynamic Routing (5p)

OSPF and RIP are dynamic routing protocols for routing within an autonomous system.

a) How does OSPF handle network topology: How does OSPF partition the network, and what are the limitations of this partitioning (with respect to how partitions are connected)? (2p)

b) OSPF and RIP use fundamentally different algorithms, but OSPF is said to *converge* faster than RIP. What does this mean, and why is this so? In your answer, you should compare the two protocols with respect to convergence. (3p)

7. DNS (5p)

a) DNS stores its data in general mapping entries called Resource Records (RRs). The following are four examples of such entries: PTR, MX, NS, SOA. What is the purpose of each entry: what mapping does each entry define (for each entry, state "from" and "to" data-type)? (2p)

b) What is a DNS domain? (1p)

c) What is a DNS zone? In particular, how does it differ from a domain? (1p)

d) What is a root server? (1p)

8. Applications: Sockets (5p)

Sketch the socket system calls of a *connection-oriented concurrent server*. You do not need to have correct data-types or error handling, just try to describe which sequence of socket system calls a connection-oriented concurrent server typically calls. You can use pseudo-code or a flow-chart, for example. An example list of system calls are the following: socket, bind, connect, accept, read, write, recvfrom, sendto, select, close.

9. Applications (5p)

a) TELNET uses a specific TCP feature to transfer high priority control data, such as ^C (control-C). Which is this feature, and why does TELNET need this feature? (2p)

b) FTP does not need to use this feature for its control messages. How does FTP solve this problem? (1p)

c) Most Internet applications encode its protocol data in clear text (ASCII/NVT), rather than in binary encoded format (such as, for example, TCP and IP). Name one advantage and one disadvantage with this solution, in comparison with binary encoding. (2p)

10. IPv6 (5p)

The IPv6 header has changed drastically from the IPv4 header. For each of the IPv4 fields below, describe what change has been made in IPv6, and why the change was made. Changes may include renaming, removal, or movement to some other header. You should be able to describe how the field has changed, with primary focus on the reason for the change.

a) Header length (1p)

b) Time-to-live (1p)

c) Protocol (1p)

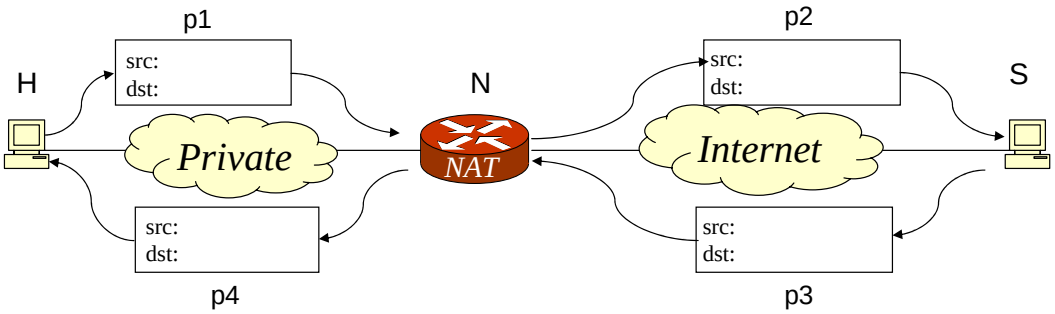
d) Header checksum (1p)

e) Options (1p)

11. Internet security (5p)

Briefly describe a typical use of digital signatures. You should describe how the sender can produce a digital signature, and how the receiver can verify it, and why the method works. You should also name which aspects of security (according to Forouzan) that a digital signature addresses. (5p)

12. NAT (5p)



A NAT/NAPT box, N, is placed between a private and public network as shown in the figure. A host, H, on the private network with address 10.0.0.23 intends to communicate with a web server, S, on the public Internet at 123.23.4.90 on port 80. The NAT/NAPT box has one public address 23.1.2.3.

a) Fill in the source and destination address and port numbers in the four positions (p1, p2, p3 and p4) as a packet is sent from the host to the web server, and the reply is sent back. In this exercise, the NAT/NAPT box should change port numbers as well – assume that the port number used by the host was already used by some other flow. (2p)

b) What is the address/port mapping that the NAT/NAPT box has after the transmission in the example? (1p)

c) What does it mean that a NAT/NAPT box is a “full cone NAT”? (1p)

d) What does it mean if the NAT/NAPT box is a “symmetric NAT”? (1p)