Closed book; no additional materials/equipment may be used during the exam.

1. Consider the network shown in Figure 1. R1, R2 are layer-3 routers. S1 and S2 are layer-2 switches. AP1 and AP2 are wireless access points, whose ranges are shown as well as the hosts connected to them. The network interface cards (NIC) have been numbered from 1 to 24. The i-th NIC is called NICi. IPi denotes the IP address of NICi (where applicable) and MACi denotes the link layer address of NICi (where applicable).

![Figure 1](image)

Figure 1: We will refer to this figure multiple times in different questions.

a) (0.4 pt) How many subnets are there in this network? Show your work by encircling each subnet (clearly show on which side of the boundary each interface is).

4 subnets as shown in the figure.

b) (0.6 pt) Hosts A (NIC1) and C (NIC21) have data packets to send to each other. Consider the journey of an IP packet travelling from host A to host C and fill in the blanks.

The destination address of the link layer frame when it is leaving R1 is __MAC4__.
The source address of the link layer frame when it is leaving R1 is __MAC3__.
The source address of the IP datagram when it is leaving R1 is __IP1__.
The destination address of the IP datagram when it is leaving R1 is __IP21__.
The source address of the link layer frame when it is leaving R2 is __MAC18__.
The destination address of the link layer frame when it is leaving R2 is __MAC21__.
2. (1.0 pt) True/False Questions - Please write down True or False. Grading: Let c, w and u denote the numbers of correct answers, wrong answers and unanswered questions, respectively, for this exercise (i.e. c+w+u=5). Rule 1: If w≥c then you gain no points from this exercise. Rule 2: If c>w, then you gain \((0.2\times c)-(0.1\times w)\) points. Example: For c=4, w=1 and u=0, you gain \((0.2\times4)-(0.1\times1)=0.7\) points.

Consider four wireless nodes, A, B, C and D shown above. The radio coverage of the four nodes is shown via the shaded ovals and all nodes use the same radio frequency range. If the destination of a message is not an immediate neighbor, then the message must be relayed. Time is slotted and transmitting a message takes exactly one time slot (other sources of delay are negligible). During a time slot, a node can do only one of the following: 1) send a message, or 2) receive a message, or 3) remain idle/silent. Assume that there are no bit-level errors. Nodes within the transmission range of a sender receive messages correctly as long as these messages do not collide with messages of other senders.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Maximum data rate, at which a data message can be transferred from C to A, given that there are no other message transmissions from other nodes, is 1 message per time slot.</td>
<td>False</td>
</tr>
<tr>
<td>b) Suppose A sends messages to B, and D sends messages to C at the same time. Collision is observed during message transmission.</td>
<td>False</td>
</tr>
<tr>
<td>c) Assume that each node transmits a message in each slot with probability (p). The probability that node B transmits successfully is (p(1-p)^2).</td>
<td>True</td>
</tr>
<tr>
<td>d) Assume that each node transmits a message in each slot with probability (p). The probability that node A transmits successfully is (p(1-p)^2).</td>
<td>False</td>
</tr>
<tr>
<td>e) Suppose that A sends messages to B and C sends messages to D. The combined maximum data rate at which data messages can flow from A to B and from C to D (the sum) is 2 messages per time slot.</td>
<td>False</td>
</tr>
</tbody>
</table>

3. (0.9 pt) Suppose within your web browser you click on a link to obtain a webpage. The IP address for associated URL is not cached in your local host, so a DNS lookup is necessary to obtain the IP address. Suppose that \(n\) DNS servers are visited before your host receives the IP address from the DNS service. The successive visits incur round-trip times of \(RTT_1, RTT_2, \ldots, RTT_n\). Further suppose that the webpage associated with the link contains exactly one HTML (text) object whose size is negligible. Let \(RTT_0\) denote the round-trip time between the local host and web server containing the object. Assuming zero processing and transmission time of the object, how much time elapses from when the client clicks on the link until the client receives the object?

The total amount of time to get the IP address is
Once the IP address is known, $RT_{T_0}$ elapses to set up the TCP connection and another $RT_{T_0}$ elapses to request and receive the small object. The total response time is

$$2RT_{T_0} + RT_{T_1} + RT_{T_2} + \cdots + RT_n$$

4. (1.5 pt) **Fill in the blanks** - Each correct answer is worth 0.1 pt.

a) A _TCP_ socket is identified by 4-tuple. These are 1) ___source IP address___, 2) ___destination IP address___, 3) ___source port number___ and 4) ___destination port number___.

b) In the Go-Back-N sliding window protocol, the sender is allowed to transmit multiple packets back to back (when available). However, it is constrained to have no more than a maximum allowable number, n, of ___unacknowledged___ packets in the pipeline.

c) ___Routing___ determines the path taken by packets from source hosts to destination hosts, while the task of ___forwarding___ is to move a packet from a router’s input to the appropriate router output.

d) ___Transmission delay___ is the amount of time required to transmit all of the packet’s bits into the link. It is equal to ___$L/R$___ where L denotes the packet length and R denotes the transmission rate of the outgoing link.

e) In wireless LANs, because of the ___hidden terminal___ problem, in which a node may not be aware of another node’s transmission due to some obstacles or range problems, collisions may occur but not be detected.

f) In the figure below, the IP addresses to all of the interfaces and MAC addresses to all of the adapters are shown. Suppose all of the ARP tables are up to date.

The network adapter in E creates an Ethernet frame with destination address ___88-88-88-88-88-88___. Router 2 receives the frame and extracts the datagram. The forwarding table in this router indicates that the datagram is to be routed to the IP address ___192.168.1.003___. Router 2 then creates the Ethernet packet with the destination address of ___33-33-33-33-33-33___ and source address of ___55-55-55-55-55-55___. The process continues until the packet reaches Host B.
5. 

a) (0.5 pt) The transmission rate of a computer in a 6-Mbps network is regulated by a token bucket whose size is 1 Mb (megabits). The token bucket is initially full and it is filled at a rate of 1 Mbps (megabits per sec). For how long can the computer transmit at the full network rate of 6 Mbps?

Net outflow from the token bucket is (6Mbps-1Mbps=5Mbps)
Full bucket to empty \( \frac{1\text{Mb}}{6\text{Mbps}-1\text{Mbps}} \) = 0.2 s
Thus, during the first 0.2 seconds the computer transmits at the maximum 6-Mbps rate and then it switches to 1-Mbps.

b) (0.7 pt) Consider the figure below showing packet arrivals and departures to/from a router. Consider the Round Robin (RR) service. Packets 1, 2, 3, 6, 11, 12 are class 1 packets, and packets 4, 5, 7, 8, 9, and 10 are class 2 packets. Indicate the time at which packets 2 through 12 each leave the queue. For each packet, what is the delay between its arrival and departure?

<table>
<thead>
<tr>
<th>Packet Order</th>
<th>4</th>
<th>2</th>
<th>5</th>
<th>3</th>
<th>7</th>
<th>6</th>
<th>8</th>
<th>11</th>
<th>9</th>
<th>12</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arrival time</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>5</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Departure time</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>Delay</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

6. Consider the following protocol aiming at mutual authentication of two parties by using a trusted server (S): If Alice wants to talk to Bob she sends her identity, Bob’s identity and a fresh session key \((K_{ab})\) all encrypted with the servers public key to the server. The server then sends Alice’s identity and the session key both encrypted with Bob’s public key to Bob. Bob generates a fresh nonce \((NB)\) and sends his identity and the nonce both encrypted with key \(K_{ab}\) to Alice. Finally Alice responds by sending her identity, Bob’s identity and NB (all without encryption) to Bob.

a) (0.5 pt) Give an informal protocol narration capturing the protocol described above.
1. $A \rightarrow S: \{A, B, \text{Kab}\}^{pk(S)}$
2. $S \rightarrow B: \{A, \text{Kab}\}^{pk(B)}$
3. $B \rightarrow A: \{B, \text{NB}\}^{\text{Kab}}$
4. $A \rightarrow B: A, B, \text{NB}$

b) (0.5 pt) Is initiator Alice correctly authenticated to responder Bob? (Motivate your answer)

No; no secret of Alice is ever used in the protocol so anyone can easily impersonate Alice. (Using the server is not even needed):

$M(S) \rightarrow B: \{A, \text{Kmb}\}^{pk(B)}$
$B \rightarrow M(A): \{B, \text{NB}\}^{\text{Kmb}}$
$M(A) \rightarrow B: A, B, \text{NB}$

1. $A \rightarrow S: \{A, B, \text{Kab}\}^{pk(S)}$
2. $S \rightarrow B: \{A, \text{Kab}\}^{pk(B)}$
3. $B \rightarrow A: \{B, \text{NB}\}^{\text{Kab}}$
4. $A \rightarrow B: A, B, \text{NB}$

b) (0.5 pt) Is responder Bob correctly authenticated to imitator Alice? (Motivate your answer)

Yes
- a secret of Bob is used; his private key to decrypt message 2.
- Bob’s response is fresh because it uses Kab that was created by Alice in this session.
- Bob’s response is meant for Alice because Bob can see her identity in msg 2 and no-one could change this value (not when going from A to S nor from S to B).

7. Alice, Bob, Charlie and Dave are all members of an online social website that allows them to specify a group ‘Friends’ using role based trust management (RT). Their policies are:

| Alice.Friends ← Alice.Friends.Friends |
| Alice.Friends ← Bob |
| Bob.Friends ← Alice |
| Bob.Friends ← Charlie |
| Charlie.Friends ← Bob.Friends |
| Charlie.Friends ← Dave |

Give the friends of Alice (0.2pts), those of Bob (0.1pt), those of Charlie (0.1pt) and those of Dave (0.1pt). (Note: only consider the policy not what you may think is ‘normal’ for Friends.)

(See answer test 2 question)

8. The NIST has defined requirements for different levels of authentication. In addition to the types of tokens used to authenticate and how you prove control of these tokens, authentication levels 2 and up have a requirement on another part of the process.
a) (0.3 pt) Which part of the process is meant here?

registration; while level 1 requires no identity proofing the higher levels require some form of check when the
token is assigned to the user.

b) (0.3 pt) Levels of authentication 3 and above require multi-factor authentication. Give the three
factors of authentication with an example of each.

have (eg smartcard) / know (eg password) / are (eg fingerprint)

9. Suppose we use a 128-bit block cipher in Cipher Feedback Mode (CFB) to encrypt a 10MB video file.

Encryption Schema for CFB

a) (0.4 pt) Draw the decryption schemas for CFB.

Simply change down to up arrows, rest stays the same.

b) (0.3 pt) Suppose a transmission error flips a single bit in C2. Which plain text blocks are affected?

Blocks P2 and P3.

c) (0.3 pt) In the scenario of (d); how many bits of plaintext will have the wrong value? (Shortly
motivate your answer.)

1 bit in P1, after encrypt about half the bits change if 1 input bit changes so in P2 ~64 so ~65 in total.
anywhere from 1 to 65 is acceptable answer as well.
(65 gives partial points 0.2p).

10. Suppose that over a medium shared amongst six parties each pair wants to be able communicate securely
without the others being able to eavesdrop. They have selected an symmetric encryption and a
asymmetric encryption algorithm.

a) (0.3 pt) How many different keys will they need in total if they use only the symmetric encryption
algorithm and how many if they use only the asymmetric encryption algorithm? (Shortly motivate
your answer.)

sym: # unordered pairs ie 6 * 5 / 2 (6 over 2) asym: 2 * 6 (public-private for each)

b) (0.2 pt) How many keys does a person have to store secretly in both cases above? (Shortly motivate
your answer.)

sym: 5 each (one for each other), asym: 1 own private key
They create and securely share the required keys for the public key algorithm.
c) (0.2 pt) For keys that they do not need to store secretly they still need to ensure integrity. How could they add an integrity check for a key that is not stored secretly?

Only relevant for asym; Sign with own secret key.

d) (0.2 pt) One of the parties wants to encrypt a large file so 4 of the 5 other parties can get access to it yet does not want to have to encrypt this large file multiple times. Give a method that achieves this.

Create new symmetric key and encrypt it with the 4 public keys. Then encrypt the large file with the symmetric key.

11. Lab questions

a) (0.3 pt) Name two attacks that exploit insufficient input sanitization or validation on a web service. Briefly describe the attacks (one sentence for each).

b) (0.3 pt) You receive an e-mail about a change in the exam location from someone claiming to be Jerry, signed via OpenPGP. You are unable to verify the claimed identity in person. However, you notice that the public key for this identity was signed by 100 other people. Is this sufficient evidence to trust the identity and thus the message? If yes, explain why. If no, mention additional requirements to trust the e-mail's authenticity.

c) (0.3 pt) In which network layers do the following attacks take place? (i) Port scan (ii) SQL injection (iii) IP spoofing.

a) (Pick two) SQL injection, XSS, Buffer overflow

(0.05 pt for each name, 0.1 pt for each description)

b) No. The person can generate as many public keys as they need to sign their own key. "Jerry" has to be a part of the web of trust.

(0.1 for No. 0.2 for explanation)

c) i) Transport ii) Application iii) Internet/network

(0.1 each)