INSTRUCTIONS:

(1) Answer questions directly on the examination paper.

(2) No notes, books, or other aids are permitted. No electrically operated aid devices are permitted, including, but not limited to, computers, calculators, cellular phones, pagers, or PDA devices.

(3) If the space allotted for your answer is too small, continue your answer on the back of the page, clearly indicating your answer is continued overleaf.

(4) The exam has 26 questions on 7 pages, apart from this cover page.

(5) Attempt all questions: partial marks are given for incomplete but correct answers.

(6) Numbers beside questions in [] brackets denote number of points the question is worth. This exam is out of 120 total points. You may want to prioritize your answering, choosing to do questions worth the largest number of points first.

*Good luck!*

Points distribution:

<table>
<thead>
<tr>
<th>Score</th>
<th>Question</th>
<th>Out of</th>
<th>Score</th>
<th>Question</th>
<th>Out of</th>
<th>Score</th>
<th>Question</th>
<th>Out of</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>4</td>
<td></td>
<td>13</td>
<td>3</td>
<td></td>
<td>25</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>5</td>
<td></td>
<td>14</td>
<td>4</td>
<td></td>
<td>26</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>5</td>
<td></td>
<td>15</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>5</td>
<td></td>
<td>16</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>4</td>
<td></td>
<td>17</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>6</td>
<td></td>
<td>18</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>4</td>
<td></td>
<td>19</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2</td>
<td></td>
<td>20</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>4</td>
<td></td>
<td>21</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>1</td>
<td></td>
<td>22</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>5</td>
<td></td>
<td>23</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>5</td>
<td></td>
<td>24</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
(1) [4] We know Alice can use her public key to encrypt a message she sends to Bob. What, if anything, would be different if: (1) Alice uses Bob’s public key to do the encryption? (2) Alice uses her public key to do the encryption?

(2) [5] Show how you could, using only simple parity (even or odd, your choice), transmit the three ASCII characters ‘C’, ‘a’, ‘T’ and be able, at the receiver, to detect and correct any single bit error in the message. [The ASCII codes for the letters are: 0x43, 0x61, 0x54 respectively].

(3) [5] When is an ICMP redirect message issued? What is the purpose of issuing the message?

(4) [5] In what way(s) are a bridge and a router the same? in what way(s) are they different?

(5) [4] What causes white noise? why is it called “white”? 
(6) [6] We saw several basic principles that security features are intended to support, e.g., confidentiality. Name and briefly describe three of these features (other than confidentiality).

(7) [4] URLs are widely used to access resources on the Internet. Briefly explain why URLs are not a good choice for locating a resource. Why might URNs be better?

(8) [2] In sliding window protocols, what does the window contain?

(9) [4] A packet of size $k$ bytes arrives at a router. That router needs to forward the packet over a network with an MTU of $k/2$, but the packet’s “Don't Fragment” bit is set. What does the router do?

(10) [1] Both Bluetooth and 802.11b operate in the ISM frequency band where they compete with one another. Why is this ISM frequency band chosen?
(11) [5] In an ARP packet, the fields for source and target protocol addresses are not as long as the fields for source and target hardware addresses. Which is longer? Why? What is an ARP message used for?

(12) [5] A part of a DNS table appears below.

```plaintext
<table>
<thead>
<tr>
<th>Hostname</th>
<th>TTL</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>flits.cs.vu.nl</td>
<td>86400</td>
<td>HINFO</td>
<td>Sun Unix</td>
</tr>
<tr>
<td>flits.cs.vu.nl</td>
<td>86400</td>
<td>A</td>
<td>192.31.231.165</td>
</tr>
<tr>
<td>flits.cs.vu.nl</td>
<td>86400</td>
<td>MX</td>
<td>1 flits.cs.vu.nl</td>
</tr>
<tr>
<td>flits.cs.vu.nl</td>
<td>86400</td>
<td>MX</td>
<td>2 zephyr.cs.vu.nl</td>
</tr>
<tr>
<td><a href="http://www.cs.vu.nl">www.cs.vu.nl</a></td>
<td>86400</td>
<td>CNAME</td>
<td>star.cs.vu.nl</td>
</tr>
<tr>
<td>ftp.cs.vu.nl</td>
<td>86400</td>
<td>CNAME</td>
<td>zephyr.cs.vu.nl</td>
</tr>
</tbody>
</table>
```

Using information from this table,

(i) email to users on flits.cs.vu.nl will be sent to:

(ii) how are www.cs.vu.nl and star.cs.vu.nl related?

(iii) what is 192.31.231.165?

(iv) suppose email to users at some new site, e.g., flits.ite.vu.nl, is supposed to be delivered to flits.cs.vu.nl for handling; what one line can you add to the table above that will achieve this?

(13) [3] For what purpose would someone use the SHA-1 algorithm?

(14) [4] Data to be sent over a network may be sensitive to delay or loss. Give examples of data that is sensitive to (i) delay but not loss, (ii) loss but not delay.
(15) [11] For the network shown below, use Djikstra’s algorithm to determine the best paths from A to each of the other nodes shown. Fill in the table provided with your intermediate results at each step. (You may or may not need all the rows provided in the table: use as many as you need to arrive at a correct result).

(16) [2] What is the subnet mask value if a site chooses to use 6 bits for host numbers on its subnets (you may express your answer in hex or in dotted decimal)

(17) [3] What makes SSM (Source Specific Multicast) special? i.e., different from ordinary multicasting?
(18) [10] Fill in the blanks:

1. When two 1012-byte frames collide on an ALOHA network, the number of frames successfully arriving at their destination is ________________

2. Traffic in an autonomous system is either local or ________________

3. Use of NAT (network address translation) involves rewriting fields in the IP header: the source address, the source port and the ________________

4. ________________ refers to using ATM to emulate a local area network.

5. Adelman, Rivest and Shamir developed the ________________ algorithm

6. The ISO network model has 7 layers; the Internet Protocol Suite has ________________ layers.

7. The Clipper chip provided an implementation of the ________________ algorithm.

8. Nodes on a token ring network can transmit frames only when they receive the ________________

9. “Integrated services” and “differentiated services” are two different approaches to handling ________________

10. Increasing the number of bits to hold sample values in a PCM system reduces ________________

(19) [2] RIP and OSPF are two different routing protocols. Each uses some measurement or metric to tell how ‘good’ a route is. What metric does RIP use? What metric does OSPF use?
(20) [5] Streaming audio players require audio data to be delivered from the Internet at a ‘steady’ rate. But, for various reasons, e.g., congestion, the delivery of data may vary in rate. That is, the delay between arrival of successive packets can vary, yet the audio player must deliver data to your ears at a constant rate. Briefly explain how streaming audio tries to maintain a constant data delivery rate to your ears while coping with variable rate data delivery from the network. [Hint: think about what leaky buckets do] {Bonus: what is the name for the phenomenon of variable delay in the arrival rate of packets?]

(21) [4] Of the five services classes supported by ATM (CBR, RT-VBR, NRT-VBR, ABR and UBR) which would the most appropriate choice for each of the following services?

- email traffic
- file transfers
- voice channel for telephony
- web surfing

(22) [5] Network security threats fall into several categories; one of these is a replay attack. Briefly explain what this attack is.

(23) [1] SMTP is a protocol used to exchange email traffic between servers. Name one of the protocols a client uses to retrieve email messages from an email server. [Bonus point for naming two such protocols]

(24) [1] A Huffman code replaces letters with variable length bit strings; the bit string for a particular letter is determined with a tree-building algorithm and information about the frequency of occurrence of the letters to be encoded. If the frequency of occurrence of letters is: W 0.50, X 0.30, Y 0.15 and Z 0.05, with which letter will the shortest length Huffman code be associated? Note that you do not need to generate the tree to answer the question.
(25) [15] Indicate whether each of the following statements is true or false:

1. Routing and forwarding are the same: ___

2. Once a packet is fragmented to accommodate a network with a smaller MTU, it can never be further fragmented: ___

3. ATM is designed to handle both real-time and non-real-time traffic: ___

4. Both ESP and AH provide encryption protection for all of the packet’s data: ___

5. There is a direct relationship between the parts of a dot separated name and its corresponding dotted decimal IP address: ___

6. The algorithm for computing cyclic redundancy checks (CRCs) is computationally expensive and complex: ___

7. In TCP, sequence numbers are assigned to individual bytes instead of to packets: ___

8. Use of NAT can provide firewall protection: ___

9. The bit rate on a link may be higher than the baud rate: ___

10. An analog signal is sampled 10,000 times per second; the digital version then correctly represents components of the signal up to 5 kHz: ___

11. Authentication is concerned with ensuring that a transmitted message has not been modified during transmission: ___

12. ADSL is a good connection scheme for operating web servers from your home: ___

13. The compression effectiveness of RLE compression depends largely on the data to be compressed: ___

14. Encryption keys are often distributed using encrypted messages: ___

15. In a packet-switched network, individual packets of a message may follow different routes through the network to their destination: ___

(26) [4] Suppose an IP packet has just arrived at a router with a time to live (TTL) field of 1. What does the router do with this packet? How would what the router does be any different if the TTL field had been 2 when the packet arrived?