INSTRUCTIONS:

(1) Answer all 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) Some questions ask for “one sentence” descriptions or explanations. Be aware that if you write more than one sentence, only the first sentence will be graded.
(5) Unless otherwise noted, all references to IP refer to IPv4.
(6) The exam has 29 questions on 7 pages, apart from this cover page.
(7) Attempt all questions: partial marks are given for incomplete but correct answers.
(8) Numbers beside questions in [] brackets denote number of points the question is worth. This exam is out of 151 total points.

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>5</td>
<td>_____</td>
<td>11</td>
<td>5</td>
<td>_____</td>
<td>21</td>
<td>10</td>
</tr>
<tr>
<td>_____</td>
<td>2</td>
<td>5</td>
<td>_____</td>
<td>12</td>
<td>3</td>
<td>_____</td>
<td>22</td>
<td>6</td>
</tr>
<tr>
<td>_____</td>
<td>3</td>
<td>6</td>
<td>_____</td>
<td>13</td>
<td>5</td>
<td>_____</td>
<td>23</td>
<td>3</td>
</tr>
<tr>
<td>_____</td>
<td>4</td>
<td>5</td>
<td>_____</td>
<td>14</td>
<td>10</td>
<td>_____</td>
<td>24</td>
<td>5</td>
</tr>
<tr>
<td>_____</td>
<td>5</td>
<td>4</td>
<td>_____</td>
<td>15</td>
<td>3</td>
<td>_____</td>
<td>25</td>
<td>5</td>
</tr>
<tr>
<td>_____</td>
<td>6</td>
<td>6</td>
<td>_____</td>
<td>16</td>
<td>5</td>
<td>_____</td>
<td>26</td>
<td>4</td>
</tr>
<tr>
<td>_____</td>
<td>7</td>
<td>6</td>
<td>_____</td>
<td>17</td>
<td>5</td>
<td>_____</td>
<td>27</td>
<td>4</td>
</tr>
<tr>
<td>_____</td>
<td>8</td>
<td>4</td>
<td>_____</td>
<td>18</td>
<td>10</td>
<td>_____</td>
<td>28</td>
<td>5</td>
</tr>
<tr>
<td>_____</td>
<td>9</td>
<td>3</td>
<td>_____</td>
<td>19</td>
<td>5</td>
<td>_____</td>
<td>29</td>
<td>5</td>
</tr>
<tr>
<td>_____</td>
<td>10</td>
<td>4</td>
<td>_____</td>
<td>20</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
(1) [5] A NAT gateway with IP address 129.174.1.13 receives from a host on the LAN for which it is the gateway a request containing this information:

<table>
<thead>
<tr>
<th>src addr</th>
<th>src port</th>
<th>dest addr</th>
<th>dest port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.5</td>
<td>x</td>
<td>132.160.81.2</td>
<td>80</td>
</tr>
</tbody>
</table>

Show what this information would look like on the 'other side,' i.e., the Internet side, of the NAT gateway:

<table>
<thead>
<tr>
<th>src addr</th>
<th>src port</th>
<th>dest addr</th>
<th>dest port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(2) [5] What will happen to performance on an Ethernet as one continues to add more and more hosts to it? How would moving to a faster Ethernet affect this trend?

(3) [6] What is a piconet? Briefly describe the structure of a piconet, answering: maximum size of a piconet, number of piconets a 'host' may join.

(4) [5] PHB has just heard about multicasting, but doesn't see why it's any different than doing multiple unicast, one to each target recipient; he asks you to explain. What do you tell him? Is it the same? If not, what's different?

(5) [4] Suppose you need to represent an image (e.g., a photograph) digitally. Briefly describe the two factors that determine the size of the file holding the digitized image.
(6) [6] Reading an RFID tag means getting from the tag information it transmits. Yet, nearly all RFID tags have no battery, hence have no power — why is this the case? How, then, is it possible for them to transmit a value to be read?

(7) [6] An essential component of a firewall is a packet filter. What is a packet filter? what does it actually do? Why is use of a NAT said to provide packet filtering?

(8) [4] In talking about networks, we often use the terms ‘protocol’ and ‘service.’ Briefly describe the relationship between them — are they the same thing? if not, what makes them different?

(9) [3] Knowing that Denver and Chicago are 1,500 km apart, what frequency of amplitude modulated radio signal would you use if you wanted to have exactly one cycle of carrier fill the distance between the cities? (Recall that, for radio, $\lambda = c/f$).

(10) [4] Services offering audio files over the network tend to use a compression method that is highly effective, like MP3. Why would such an effective technique not be used for applications like telephony?
(11) [5] A web server, running on a node named somenode.netlab.gmu.edu has a file /top/foo/fleebert.html. Show the URL needed to access this file. Suppose the server ran, not on the standard port, but on port 47361; show the URL needed to access the file in this case. What is the standard port number for a web server to run on?

(12) [3] Briefly explain the main distinction between HTML and XML.

(13) [5] In settings requiring delivery of real-time, mission-critical data, common wisdom is to use high bit-rate networks. Consider, for example, use of a 100 Mbps Ethernet for such data. Is this speed good enough to ensure real-time delivery of mission-critical data? why or why not? would a faster Ethernet be better?

(14) [10] Usually, the From: line in an email header is simple plain-text, and consequently easy to read. Explain why the From: line shown below is so much more complicated (note you are not being asked to decode the line):
   From: =?ISO-8859-1?q?Patrik_F=E4ltstr=F6m?= <paf@nada.kth.se>

(15) [3] Given that TCP provides reliable transport whereas UDP does not, why does the protocol used for VoIP use UDP? What is the name of that protocol?

(16) [5] PHB is concerned that users can be confident of the authenticity of information and software downloads from the company website. What solution can you suggest?
(17) [5] Suppose we record a live concert digitally. We sample the analog audio 48,000 times per second and represent the measured value using a 4-bit number. The result sounds terrible — why? What, if anything, should we have done differently?

(18) [10] State whether each of the following statements is true or false:

(i) UDP performs no fragmentation nor reassembly of messages

(ii) Some RFID tags can be read by low orbitting satellites

(iii) MD5 and SHA-1 are the same kind of algorithm, but produce different results

(iv) MD5 and SHA-1 are the same kind of algorithm, but produce different results

(v) When performing MPEG compression, audio and video components are compressed independently

(vi) Lines in an email message header are required for SMTP to deliver the message

(vii) IP addresses can be re-used when DHCP is used to assign host addresses

(viii) Bluetooth supports both connection-oriented and connectionless service

(ix) The text of client messages to a server can only be 7-bit ASCII:

(x) Use of HTML completely specifies the layout and appearance of a web page

(19) [5] A resolver is software whose job is to produce an IP address given a host name, using the DNS. Resolvers may operate in either recursive or iterative modes. Briefly explain the difference between these two and the role they play in resolving names to addresses.
(20) [5] What is a denial of service attack? how is a distributed denial of service attack different? Suggest two countermeasures we saw to mitigate such attacks (hint: for one of these think about what role routers play in a DDOS).

(21) [10] Fill in the blanks:

Which of 802.11b or 802.11g supports higher bit rates: ________________

Host address + port number = ________________

The maximum size of an IP datagram is ________________

The 16-bit character code suitable for any written language is ________________

The TLD in foobert.gmu.edu: ________________

Protocol used by signalling gateway in VoIP: ________________

Which of 802.11b or Bluetooth has greater range: ________________

Kind of attack that IPsec's AH guards against: ________________

An open source network security monitoring application: ________________

To be useful, a router must have at least ________________ Internet addresses.

(22) [6] PHB is frustrated, and so has called you. He types in a URL to his web browser and gets back a message indicating 'host not found.' Assume that PHB made no mistake typing in the URL and that it is correct. What do you suspect is wrong? What steps do you take to identify the problem? How do you determine is the problem is internal (to the organization's network for which you are responsible) or external?
(23) [3] Is there any difference if a shopper buys an item identified with a UPC bar-code symbol or with an RFID tag?

(24) [5] PHB takes his wireless notebook to his favourite Internet Café and gets on their network. Suppose his notebook has an application that shows when a port receives a request (irrespective of whether there is actually a service available there). PHB notices that the port where a web server would run (he doesn't run one on his notebook) is getting dozens of requests. He asks you to explain why this is so; what do you tell him has likely happened?

(25) [5] URLs are often described as being “brittle” — why? Suggest an alternative that would not have this weakness, explaining why it is better than a URL.

(26) [4] Confidentiality is an area of network security that everyone thinks of. We saw, though, that there are other factors to consider when thinking of security: name and describe two of these.
(27) [4] In examining on-going operating costs for an installation, “vendor churn” is cited as one of the negatives for proprietary solutions (as opposed to open source). What is vendor churn, and how does it affect operating cost?

(28) [5] Two nodes that want to establish encrypted communication between themselves often begin their interaction using one encryption technique, then almost immediately switch to another. Why do they do this? What encryption technique did they start with and which do they switch to?

(29) [5] For each of the names or terms appearing on the left, provide at most a one sentence description of what the name or term means (if the term is an acronym, expand the acronym as part of your answer):

1. X.509
2. SNMP
3. 802.3
4. OC3
5. SLP