COMP28411 Examination Performance Feedback

2013-2014

Fact that majority of students chose not to attend lectures was very evident in answers given in the examination.

Question 1

a) This part was about gathering information that the model/router could not know but which it required, i.e. next hop gateway and IP address of a DNS server.

The question stated that the IP address was supplied and asked for two other pieces of information, hence, IP address was not a valid answer. A subnet mask may be supplied but is not required, so this is only partially correct. Port numbers are well known or dynamically allocated by the operating system, thus they do not need to be supplied by the ISP. Things like its MAC address are built into the interface card of the router and do not need to be discovered. The physical cable, although often supplied by the ISP, is not information, which the question explicitly asked for.

b) This part was about how the NAT performed the translations necessary for private addresses to communicate with the wider Internet. Hence, looking for what translations are performed when a packet is sent and received. Also what information has to be remembered from sending a packet to allow the translation of a reply packet.

Many of the answers given lacked detail. Saying that it did translation merely indicated that you could spot one of the words in the question.

c) This part was an application of the process worked though in the second workshop. A block of class C addresses needs to be allocated to each physical network, where the block size must be 2^N, i.e. 1, 2, 4, 8, …. Each block also needs to start on an address boundary so that a single netmask can be used to distinguish all of this block from all other addresses, i.e. the start address of the block must be divisible by 2^N where N is the size of the block.

The question asked for working to be shown so that marks could be awarded for approach when incorrect allocations where given, frequently no working was shown in answers. A significant number of answers allocated blocks that were not 2^N in size and/or which did not start on a 2^N boundary. Some answers allocated the same address to different physical networks and many answers failed to answers the what netmask should be used for each physical network part of the question.

d) This part was looking for students to identify that the service model is about what a layer does and that it is used by the next layer up to implement its own what it does.

Too many answers described the service model as about being the how (implementation) of a layer rather than the what of a layer. Given that the role in the stack is about the interaction between layers, a significant number of answers incorrectly described it as about the interaction between the ends of a communication.

e) This part was looking for a few basic service model characteristics of the two protocols to be identified, e.g. reliable/unreliable, sequenced/unsequenced and flow controlled

The lack of understanding between the what and how of the previous part was also evident here. Too often implementation details like sequence numbers were described as part of the service model of TCL; sequence numbers are the way in which TCP implements service model features like reliability. A significant number of answers described UDP as fast. There is nothing in its service model and bandwidth or delay guarantees, which would be the service model features equivalent to this. In practice, because it does not implement the reliability of TCP, it is faster than TCP, but this is not a characteristic of its service model. Several answers claimed that TCP was secure, which it is not.

f) This part was looking for a simple statement that variable sized windows are associated with flow control part of a service model. It also asked for details of the packets sent from the transmitter to the receiver and the acknowledgements from the receiver to the transmitter for the given scenario.

A significant number of the answers incorrectly stated what part of the service model a fixed sized sliding window implements. A number of answers claimed that no terminating condition was given, which was incorrect. As the receiver had a buffer for six packets and the receiving application only consumes three packets, the maximum number of packets that could be sent was nine; after these have been sent, the system is stable and no further activity occurs. The question asked for details of acknowledgements sent to include the acknowledgement number and window size, a significant number of answers lacked any information on the window size. A number of answers failed to indicate clearly how the transmitter would know that additional space was available in the receiver's buffer at time four. There is nothing in the question that restricts the sending of packets to one each time slot and the answers assumes that multiple packets can be sent at the same time. A number of answers assumed that only a single packet could be sent in each time slot.

Question 2

a) This part was looking for a statement of the two approaches, implicit or explicit data typing (calling these canonical and receiver makes right, would be fine), and an outline of how these operated by just knowing what was expected or having explicit type markers in the data sent.

Some answers just said that the receiver makes right without stating how it would know what it had received. Others answers indicated that the canonical approach always required two translations, whereas, this is the worst case situation. A significant number of answers indicated that checksums should be used to know how to interpret the data; checksums are about knowing when data has been corrected/alter not how to interpret it.

b) This park was looking for a description of the process that ensure that unique names are allocated to individual organisations/machine and the process via which the lookup of a name occurs.

Also all answers concentrated on the lookup process and gave no description of the allocation process. Where the allocation process was described if was often just given as delegation without an indication of how unique prefixed for organisations are ensured.

c) This park was looking for four good or bad points about the packet format in relation to extensibility to be given, e.g. operation not fixed (good), only single parameter (bad).

Frequently the points made in answers were just general comments that had no relationship to extensibility. For example, "there is no checksum" and "there is no indication of port". In the case of the comment about the lack of a port number, apart from not relating to extensibility this is a concern of a level below the application level. Some points made where also incorrect, "the length field means that the packet length is fixed". If the packet length was fixed there would be no need for a length field to tell the receiving side how much data has been sent.

d) This part was looking for three contrasting points about the use of symmetric and non-symmetric encryption, e.g. encryption/decryption speed and non-repudiation only possible with non-symmetric keys.

Many answers gave symmetric encryption/decryption fast and non-symmetric encryption/decryption slow as two points; this is a single point. A significant number of answers also claimed that symmetric encryption was less secure than symmetric encryption, which is not true. If it was, why would be majority of systems that protect the transmission of data be based on symmetric keys.

e) This part was looking for the use of symmetric keys to protect the transmission of the file, because it is much faster than non-symmetric. This means that a session key must be generated and securely sent using the existing non-symmetric (public/private) keys. The need for Bob to the able to verify the sender means that Alice will need to produce a digital signature for the file encrypted with her private key.

Several answers suggested encrypting the whole file with Alice's private key; this is too computationally expensive to be practical. Other problems with solutions include encrypting the message with both the public and private key before sending, which means that the file is sent in plain text; using Bob's public key in the process to prove that Alice is Alice, but anyone could do this not just Alice; encrypting the session key with Alice's private key for transmission, but then anyone can decrypt and get the session key; encrypt session key with Bob's public and Alice's private, this does not prove Alice is Alice as Bob has no value to compare session key to; encrypt file with Alice's private key, not prove Alice is Alice as no value to compare decrypted file to; use TLS, explicitly ruled out in question. Some answers suggested using a three-way authentication before sending the file using a session key. Although this works, it requires more transfers than is necessary.

Question 3

a) Overall this part of the question was well answered.

The most common points that were discussed were: no missing data, sequence numbers, connection set-up, and error free.
Whereas only a couple of students discussed the points that: data is delivered as a raw byte stream, and TCP decides when to transmit data.
A fair number of students also discussed TCP being unicast and the use of Acknowledgements in more detail.
A good proportion of students also discussed congestion control, however roughly half of these answers were unclear or more commonly seemed to confuse congestion with flow control.
In addition quite a few student's answers suggested that they were not aware that data is only delivered in order.
Marks were generally lost because of poor/short reasons, quite commonly a student would classify a point made as “both” but then only explain the advantages.
And a small number of students were given low marks simply because they didn't give any reasons or because they did not give enough points.

b) Overall this part wasn't answered well.

Most students failed to use their knowledge of UDP/RTP/RTCP to suggest extensions.
A number of students highlighted the reasons why TCP is a bad choice of protocol, but did not suggest any extensions.
A good proportion of students that didn't discuss UDP, RTP, or RTCP suggested sensible improvements, but could not suggest more than a couple of points.
Most of the students that used their knowledge of UDP/RTP/RTCP gave good answers, with only a small number of these losing marks either for not explaining how the extra data could be used or because they didn't specify what additional data was needed.

Question 4

Only seven students chose to answer this question and overall it was answered very poorly. In a few cases, this appears to be because the student ran out of time to answer fully.

a) The students that answered this part generally knew a few advantages of using PPP, however for the most part they didn't reason why PPP “over” ATM or Ethernet.

And they also didn't reason about why you couldn't just use straight Ethernet.

b) Whilst most students correctly knew how to find the start of an Ethernet frame, almost all students didn't know how the end of an Ethernet frame is found. The common misconception being that there is a sentinel at the end.

c) This part was badly answered, a lot of students either didn't give a reason “why?” or their reason wasn't sensible.

d) Again quite a few students did not answer this question at all, those that did generally only answered part ii), however the students that did attempt to answer the question generally could answer part ii) well but answered part i) badly.