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

Question 1
a)This question was asking why it might be necessary to convert data in a computer network. For example, integers may be stored/represented differently on different nodes.
Some answers lost a mark because they simply said to change data without giving any reason why this might be necessary. Others indicated that data conversion was adding and removing fields, which it is not. Finally, come answers said that it was encryption/decryption which again it is not.
b)This was looking for some details of how the two approaches work with an example of each.
A significant number of answers lacked detail, while other lacked examples. For example, many answers did not show how in a receiver makes right approach, the receiver would know what it had received. A number of answers stated that in a canonical approach two transformations were always required, when in fact at most two translations will be required.
c)This answer required a simple explanation of what extensibility was and why is important.
Although many answers correctly described what extensibility is, they failed to describe why it is important. A significant number of answers confused scalability with extensibility. Extensibility allows functionality to be added to an application, scalability allows the number of instances of an application to be increased.
d)This answer was looking for examples of extensibility in both Telnet and HTTP, and information on how this extensibility might be used.
A significant number of answers failed to give examples of extensibility in both Telnet and HTTP. Even more failed to give an example of how the extensibility might be used.
e)This question required the prevention of tampering of non-confidential data, while maximising the security of the existing keys.
A number of answers suggested encrypting the whole message, which requires unnecessary work. Some answers failed to attach an encrypted checksum, which means that there was no way of ensure that the message had not been altered (an encrypted message can be altered). Most answers used Alice's and Bob's existing keys to encrypt the checksum, which does not maximise the security of these keys. The marking scheme expected the creation of a session key that that exchanged using the existing keys and then used encrypt the checksum. One answer suggested sending both an encrypted and non-encrypted version of the message; it is not clear how this would have prevented tampering.

Question 2
a)This part was looking for information on how the three approaches worked when there was no error and when there was an error.
The descriptions given were reasonable. However, in practice six descriptions were needed and most answers did not give the complete set.
b)This question was looking for the three approaches to be compared and contrasted (pros and cons given) on two criteria. It also asked for factors that would affect the answer.
The answers generally lacked some detail. In particular, generally answers did not discuss on how the rate at which errors occur effects which of the approaches have the lowest overheads.
c)This part was asking for information about when flow control is important. As an end-to-end function, flow control relates to data not arriving at a receiver when its buffers are full.
Too many answers indicated that flow control related to congestion in the network, as congestion in the network has nothing to do with the state of receiving buffers, this is not correct.
d)This part was looking for information about how a sliding window indicates the range of data can be sent to a receiver. It was also looking for how flow control adapts the fixed size window to one whose size can be varied.
Answers were generally correct in the description of what a sliding window is. However, most failed to indicate that in flow control the size of the window can be changed.
e)This part was looking for information about what messages would be sent across the network. Given that this relates to flow control, the generic description of the messages should include the size of the window. It was also the case that the system was state at time 0, so nothing will happen until data is removed from the receive buffer.
A number of answers assumed that messages started to be transferred at time 0. As the system is stable and no space has been created in the receive buffer, this cannot occur. Other answers sent data of the transmitter at time 3 when data is removed from the receive buffer. As there is no way for the transmitter to be aware of the change in the state of the receiver, this cannot occur. The final common problem was to send data from the transmitter one byte at a time. As this is very inefficient, it will not be done. The transmitter will send a number of bytes equal to the space in the receive buffer as indicated by the window size attribute in the message from the receiver to the transmitter.

Question 3.
This question produced a wide variety of different quality answers but the fact that most students answered the TCP part of the question quite well but were much weaker on the rest of the question suggests too much reliance on general networking knowledge.

Part a:: Several people gave answers only referring to global routing of multicast packets. Clearly a lot of students had not understood the differences between unicast and multicast transport.

Part b: Almost everybody did a good job of answering this part showing a clear comprehension of the differences between live and non live streaming and the tradeoffs between using TCP and UDP multicast. However, a few still seem to think that multicast TCP exists.

Part c: Most did well on this but a few had no idea.

Part d: It was clear that many students have no idea what a hub is/was.

Part e: Too many answers seemed to be saying that 2 separate addressing schemes are used because it is not possible to deliver traffic to a host computer using just its IP address. To some extent this is true but it is true because IP mixes location specification with ID whereas MAC addresses are only an ID. Having a 2 layer addressing scheme has to a large extent enabled the proliferation of devices we now see.

Quesiton 4.
Most answers to this question were good. However, a number of students clearly had little or no idea about this part of the course.

Part a: Mostly answered well.

Part b: The importance of giving a fair share of resource to all types of traffic was well appreciated in almost all answers.

Part c-e: The use of token buckets to limit average throughput for traffic but allowing some bursts of traffic was well presented by most with appropriate illustration. A minority though seemed to think that token buckets are effectively queues of IP packets rather than a conceptual model for controlling the forwarding of incoming packets towards the output stages of a router.

Part f: This partly tested knowledge of what would happen in a saturated overload of input packets situation using token buckets. Most answers predicting correctly that initially everything simply gets forwarded for a short time until the buckets empty. This initially may appear unfair. Token buckets control and limit throughput they do not impose fairness. Normally, a Weighted Fair Queue (WFQ) imposes a fair division of what gets sent when between the variety of input streams for the router's output traffic.