CITS3002, Computer Networks, S1-20 FINAL

1. Q1a - 10 MARKS

With reference to the traditional stop-and-wait protocol, consider a variant of this protocol that uses only negative acknowledgments (NACKs), and no positive acknowledgments (ACKs).

Describe what timeouts would need to be managed, by both the sender and receiver, in such a NACK-based protocol.

Under what circumstances would we expect a NACK-based protocol to perform better than an ACK-based protocol?

(Please write your essay question on a separate piece of paper)

2. Q1b - 10 MARKS

With reference to at least four points, explain how the TCP/IP protocol suite has been able to successfully support the explosive growth in the number of hosts on the Internet.

(Please write your essay question on a separate piece of paper)

3. Q2a - 10 MARKS

IPv4 addresses were originally divided into separate classes to partition them into different sized blocks for use by different organisations. This system was then replaced with a more flexible mechanism to partition the addresses of IPv4.

Describe how the original class-based addressing scheme was used, the representation of the addresses in IPv4 packets, and the problems that were caused by adopting the original approach.

Describe the new system that replaced the original one.

What are the advantages of the new approach?

(Please write your essay question on a separate piece of paper)

4. Q2b - 5 MARKS

With reference to two examples, explain the relationship between the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP).

(Please write your essay question on a separate piece of paper)

5. Q2c - 5 MARKS

Both UDP and TCP employ port numbers to identify the destination entity when delivering a message.

Give two distinct reasons why these protocols introduced a new abstract identification value (the port number), instead of using process-identifiers (PIDs), which already existed when these protocols were designed.

(Please write your essay question on a separate piece of paper)

6. Q3a - 10 MARKS

Consider the delivery of messages in an internetworked environment, in which the source and destination nodes are many hops apart. Large messages must be fragmented and reassembled using one of two possible approaches.

- The first approach involves fragmenting each message at the source node, and then reassembling them at the destination node.
- The second approach involves fragmenting each message at the source node, reassembling and re-fragmenting them at intermediate nodes, and final reassembly at the destination node.

With reference to two distinct examples, describe circumstances where each method would be preferred over the other.

(Please write your essay question on a separate piece of paper)

---

7. Q3b - 10 MARKS

Consider the following design of an IP-based Internet chat system that permits multiple users to converse using single-line text messages:

- A chat monitor resides at a well-known network address, uses UDP to communicate with chat clients, sets up chat servers for each chat session (a chat room), and maintains a chat session directory.
- A chat server uses TCP for communication with clients.
- A chat client allows users to list all chat sessions, and to start, join, and leave any chat session.

Present, using pseudo-code with a syntax similar to either Java, Python, or C, your design of the Internet chat system.

In your pseudo-code, use uppercase letters to highlight all calls to functions provided by the Berkeley sockets API.

(Please write your essay question on a separate piece of paper)

---

8. Q4a - 10 MARKS

The Network File System (NFS) employs Remote Procedure Calls (RPCs) over the User Datagram Protocol (UDP).

With reference to traditional file-system semantics, what problems does this choice of transport-layer protocol introduce?

What solutions have been implemented to address these problems?

(Please write your essay question on a separate piece of paper)

---

9. Q4b - 10 MARKS

The Address Resolution Protocol (ARP) associates physical hardware addresses with IP addresses. This association may change over time. Each node in a local-area network maintains an ARP cache mapping corresponding IP and hardware addresses. A node trying to find the hardware address for an IP address that is not in its cache, broadcasts an ARP request that also contains its own IP and hardware addresses. The node with the requested IP address replies with its hardware address.

What are the possible vulnerabilities for spoofing in the ARP protocol?

What defences can be employed against ARP spoofing?

(Please write your essay question on a separate piece of paper)