2006

Question 1 **[30 marks]**

(a) [2 Marks] Why are iterative DNS queries perfered over recursive queries.

Load on servers

(b) [2 Marks] What is a cononical name with respect to the DNS.

The real name, used when specifying an alias.

(d) [2 Marks] What is meant by an impure name.

One that includes location information (e.g. host, directory)

(e) [4 Marks] How is a digital signature generated?

Hash -> private key -> cert. Can be checked with public key by anyone.

(f) [2 Marks] Why does an email client send outgoing email to its SMTP server rather than directly to the recipient's SMTP server?

So the client can disconnect if the server is not available.

(g) [3 Marks] What is a "protocol"?

(h) [4 marks] Briefly describe congestion control and its key parameters in TCP.

Congestion refers how TCP deals with network packet loss/delay. Parameter "congestionWindow" identifies how many MTU can be transmitted within a "round". If failure is detected through lost packet – three duplicate ACKs are sent from receiver, requiring congestionWindow to halve and set threshold to half its current value. A timeout requires the congestion window to go back to 1 and threshold to be halved.

(i) [4 marks] Briefly describe the operation of the data link control mechanism CSMA/CD.

Carrier sense, check to see if someone is transmitting already and wait for them to finish. Multiple access, allows a distributed access to the medium only requiring local control. Collision detection (if signal not identical to transmitted signal then two devices have transmitted within collision window)

(j) [3 marks] What features make RTP particularly suitable for real time transport such as voice or video?

Type of stream being transmitted is identified, timestamp of the first byte of the sample is provided, plus source identifier and sample sequence number.

(k) [4 marks] Describe how jitter is removed from streaming multimedia?

Receive buffer is the crucial component, buffer size depends on delay and jitter as well as the end to end protocol (TCP or UDP), use an adaptive smoothing technique for optimising jitter removal.

Question 2 **[30 marks]**

(a) [4 Marks] Explain the following terms

i. Cryptogrpahy

Conceled Meaning

ii. Steganography

Hidden Writing

(b) [4 Marks] What is the difference between Transposition and Substitution Cyphers?

Transposition: Swap positions, letters retain value.
Substitution: Swap value, letters retain position

(b) [2 Marks] What type of alphabetic cypher is a Ceaser Cypher?

Monoalphabetic

(c) [2 Marks] What type of alphabetic cypher is a Vigerne Cypher?

Polyalphabetic

(d) Cryptanalysis

i. [5 Marks] Identify and outline the technique devised by Al-Kindi that is best used to crack a Ceaser Cypher?

Freq analysis

ii. [3 Marks] How was this method modified by Babage to crack the Vigenere Cypher?

Modified to determine the key length and thereby treat the message as a set of monoalphabetic ciphers that can be cracked via standard frequency analysis.

(i) Authentication

i. [3 Marks] How does a nonce solve the problem of a replay attack.

It makes the encoding of the passphase unique and therefore

not suspectible to replay.

ii. [7 Marks] Explain the key distribution problem when using public key encryption for authentication. Be sure to indicate how this is resolved by a CA.

The public key must be correctly passed from the sender to the recipient (when they have not met) without being subject to a man in the middle attack. The CA solves this by having a well known public key (included in many browser distributions) that is used to digitally sign a certificate containing the senders public key. Everyone can therefore verify the public key by checking the CA signature.

Question 3 **[30 marks]**

(a) What is the role of the transport layer?

Application to application layer communication. (lose points for saying reliable)

(b) In what way is TCP not a pure GoBackN algorithm?

It only sends the segment that timed out – also triple ack. Action of receiver in response to missing sequence is undefined by the protocol specification.

(c) Why are the Source and Destination IP addresses needed in a UDP datagram.

So the datagram can be routed to the destination, and so the source can be Identified for a reply(not mandatory).

(d) Why are the Source and Destination IP addresses needed for a TCP segment.

So that in combination with port numbers, multiple TCP streams can be demultiplexed to the correct socket.

(e) What mechanism is used to set up a TCP connection, and why is it needed?

3 Way handshake, used to prevent surious connections due to spontaneous emission of old connection requests due to the store and forward nature of packet switched networks (IP).

(f) What is flow control and how is it achieved by TCP.

Ensures the sender does not overwhelm the receiver. It is achieved by limiting the size of the send buffer (inflight segments). As the receiver generates the ACKS, the transmission is therefore throttled by its processing ability.

Question 4 **[30 marks]**

(a) [4 marks] State the primary differences between the link-state and distance-vector routing algorithms.

Link-state: global topology information known at all nodes (flooded), uses Dikjstra's algorithm to create spanning tree. Good multicast support.

Distance-vector: Bellman Ford algorithm, neighbours exchange vectors with each other only. Do not have a global view of the network, multicast can only be inferred.

(b) [8 marks] Consider a broadcast algorithm that uses link-state information to achieve broadcast delivery. Briefly discuss how a broadcast message is routed efficiently through a network using the link-state information. Given the network in figure Q.4, draw the broadcast topology from node A, given that each link has equal cost.

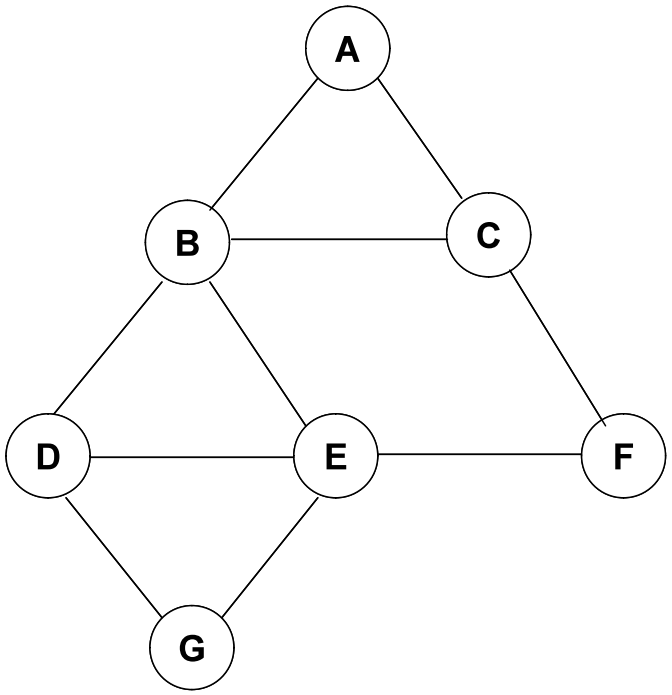
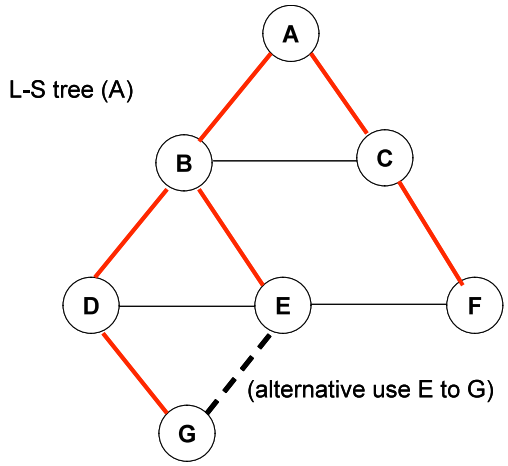


Figure Q.4

Answer:

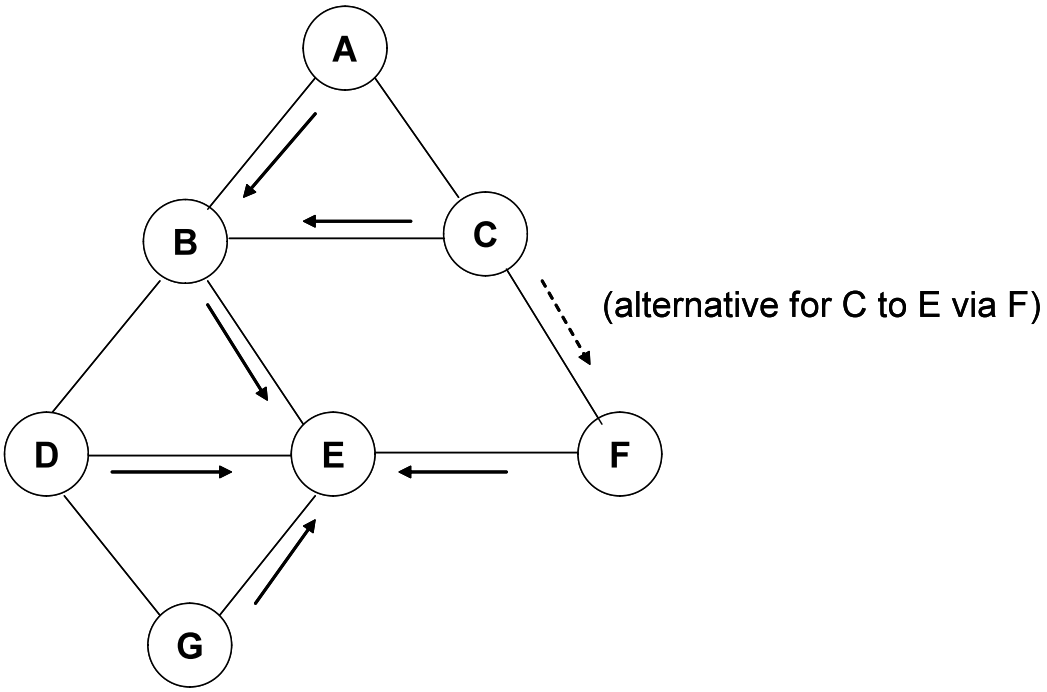
L-S uses the spanning tree developed within the L-S protocol both for forwarding unicast packets and broadcast packets. For broadcast packets the tree is flooded, so that at each node a copy of the broadcast packet is transmitted down each link in the spanning tree.



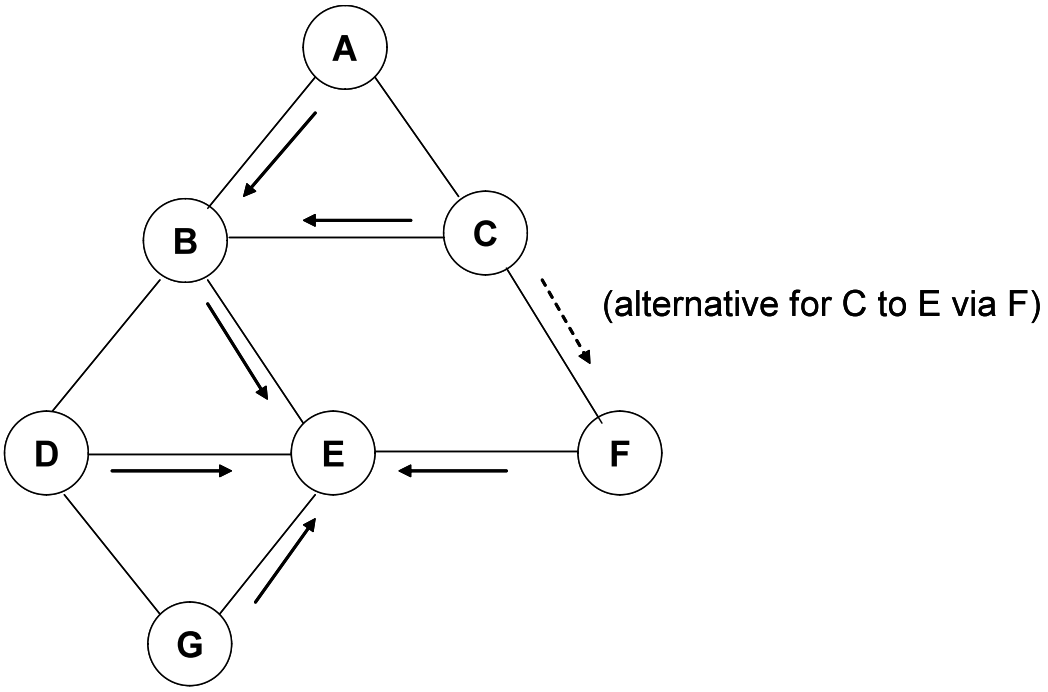
(c) [10 marks] A centre based tree (CBT) is an alternative mechanism for creating an efficient broadcast mechanism. Discuss how the CBT algorithm is used. Assume that node E is used as the core of a CBT, draw the CBT for the network shown in figure Q.4.

Answer:

CBT algorithm creates a join message which is unicast to the centre node. The unicast join is sent using the standard routing protocol information. On getting to the centre node or to a node already part of the CBT the join is actioned creating the tree.



Centre based tree on E (creation)



Centre based tree on E (creation)

(d) [8 marks] Identify the key components in Mobile IP. Discuss registration in the context of Mobile IP and how information changes as a mobile host moves from one foreign network to another foreign network.

Answer:
Home network, home agent (HA), mobile node (MN), visited (or foreign network), foreign agent (FA) and correspondent C.

Registration allows a MN to register with a FA, which then registers the presence of the MN with the HA. The information identifies the MN, the COA etc and the encapsulation used between the HA and the FA (for triangle routing).

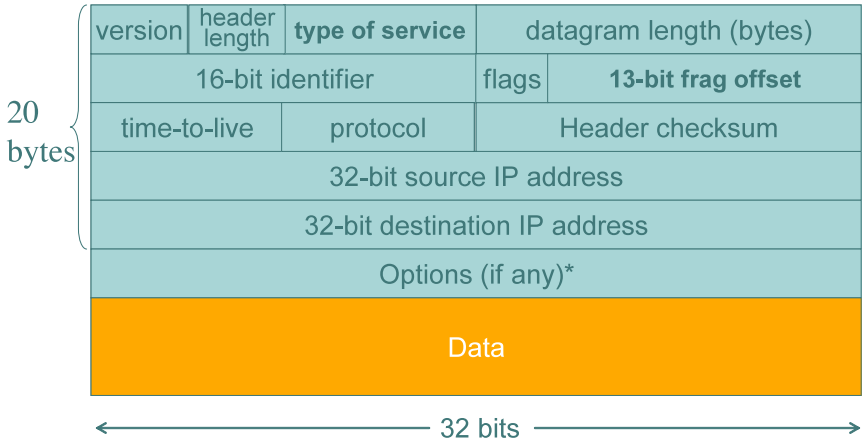
The MN on moving to a new foreign network would register with the new FA and thus the HA would be made aware through registration of the new FA and COA.

Question 5 **[30 marks]**

(a) [8 marks] What are the functions of the network layer in the TCP/IP protocol stack? In your answer you should include a brief discussion on ICMP (Internet Control Management Protocol).

(b) [14 marks] Discuss the key aspects of the Internet Protocol implemented in hosts and routers. In your answer you can refer to the IP headers for version 4 and version 6 shown in figure Q.5.

IPv4



IPv6

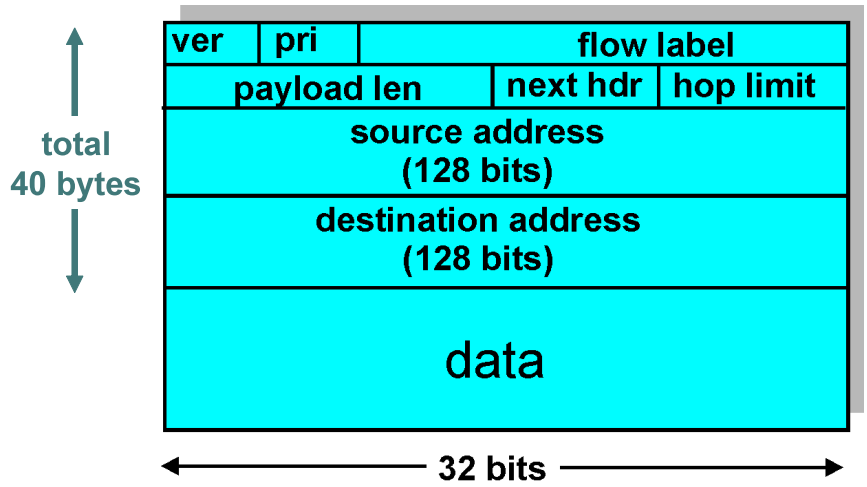


Figure Q5

(c) [8 marks] Briefly discuss the pro's and con's of Integrated Services (IntServ) and Differentiated Services (DiffServ) approaches to enabling quality of service in the Internet.