THE HONG KONG POLYTECHNIC UNIVERSITY

Department of Computing

This is a open-book examination.

(COMP5311)

Internet Infrastructure and Protocols

20 December, 2005 3.5 hours

[Answer at most 7 questions in section A and both questions in section B.]

Turn Over

Section A: Please answer ANY SEVEN questions in this section [8 marks each, making up a total of 56 marks out of 100.]

1. An MSc student Eric ran Ethereal to capture packets from a machine with IP address `158.132.11.98`, and he captured many broadcast packets, e.g., with the following addresses:

Source addresses	Destination addresses
158.132.11.89	158.132.11.255
158.132.10.51	158.132.11.255
158.132.10.65	158.132.11.255
158.132.11.70	255.255.255.255
158.132.11.61	158.132.11.255
158.132.10.27	255.255.255.255
158.132.10.123	158.132.11.255
...	...

   (a) (3 marks) What is the subnet mask of the subnet where the machine is located and why?

   (b) (3 marks) Many of the broadcast packets observed from the network were ARP request messages sent from other hosts. However, Eric did not observe any ARP replies to these requests. Please help Eric resolve this puzzle.

   (c) (2 marks) Moreover, Eric examined the ARP cache from time to time. He observed that the cache size was increasing, even though he did not run any applications. Please help Eric resolve this puzzle.

2. Answer the following questions concerning IP fragmentation.

   (a) (3 marks) What would be the values of the `Fragment Offset` and the `M` bit for an IP packet that has not be fragmented? Explain why.

   (b) (2 marks) If an IP packet, tunneled or not, has been fragmented more than once (multiple fragmentation), how many fragments that arrive at the destination for reassembly would have the `M` bit set to 0? Explain your answer.

   (c) (3 marks) What is the maximum value of the `Fragment Offset`, assuming that the MTU value can be very large and why?

3. Consider the class B IP network in Fig. 1 in which the subnet masks are all `255.255.0.0` (i.e., no subnetting). Moreover, the hosts on the subnets have only a single forwarding entry—for `140.10.0.0/16`. That is, each host assumes that all other hosts in the network are directly connected.

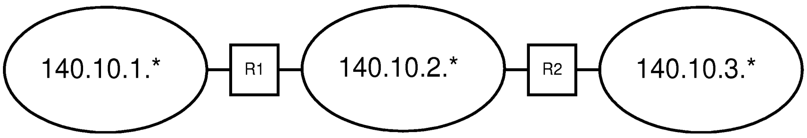


Figure 1: An IP network without subnetting.

In order to enable communications among the hosts, $R1$ and $R2$ are configured as proxy ARPs. Assume that $R1$ and $R2$ *do not* run any routing protocol between them.

(a) (4 marks) Explain in detail how $R1$ acts as a proxy ARP.

(b) (4 marks) Explain in detail how $R2$ acts as a proxy ARP.

4. Consider the following TCP packet trace between hosts A and B. The first 5 items correspond to the normal TCP close handshake. In 5.1, an old duplicated data segment arrived at A.

(a) (2 marks) What did A send back to B in 5.2 in response to an old data segment, and why?

(b) (3 marks) What did B send send back in 5.3 in response to the packet sent from A in 5.2, and why?

(c) (3 marks) What is impact of the old duplicate TCP segment on this TCP connection, and why?

```
        TCP A                                                 TCP B
1.  ESTABLISHED                                            ESTABLISHED
    (Close)
2.  FIN_WAIT_1  --> FIN segment: SEQ=1100, ACK=1300       --> CLOSE_WAIT
3.  FIN_WAIT_2  <-- Pure ACK: ACK=1101                    <-- CLOSE_WAIT
                                                               (Close)
4.  TIME_WAIT   <-- FIN segment: SEQ=1300, ACK=1101       <-- LAST_ACK
5.  TIME_WAIT   --> Pure ACK: ACK=1301                    --> CLOSED
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
5.1 TIME_WAIT   <-- Old duplicate data: SEQ=1255, ACK=1033
5.2 TIME_WAIT   --> ???                                   -->
5.3             <-- ???                                   <--
```

5. Since the TCP RESET segment can be used to reset a TCP connection, it has to be designed carefully. The current standard requires the `RST` segment to be processed as follows.

   - If the `RST` bit is set,
     - If (`RCV.NXT` <= `SEG.SEQ` < `RCV.NXT+RCV.WND`)
       - Reset the connection.
     - else
       - Silently drop the `RST` segment.

   Now consider an attacker, who knows the socket addresses of an active connection, and he blindly sends `RST` segments to either side. Moreover, he spoofs the source addresses in the `RST` segments, i.e., the source addresses are fake.

   (a) (2 marks) Is the attack more effective with a larger `RCV.WND` or a smaller `RCV.WND`? Why?

   An engineer proposed the following modification to the processing of `RST` segments:

   - If the `RST` bit is set,
     - If the sequence number exactly matches the next expected sequence number, i.e., `RCV.NXT` = `SEG.SEQ`.
       - Reset the connection.
     - else if `RCV.NXT` < `SEG.SEQ` < (`RCV.NXT+RCV.WND`)
       - Send an ACK with a value of `RCV.NXT`.
     - else
       - Silently drop the `RST` segment.

   (b) (3 marks) What is the impact of this modified algorithm on legitimate `RST` segments? Explain your answer.

   (c) (3 marks) What is the impact of this modified algorithm on `RST` segments sent from an attacker? Explain your answer.

6. Consider Fig. 2 for the data transmission in a TCP connection. Similar to problem 3 in assignment 2, each ACK value in the graph is set to the sequence number of the last byte in the acknowledged data segment. There are two packet losses occurred to this connection, and the second one occurred to the retransmitted segment.

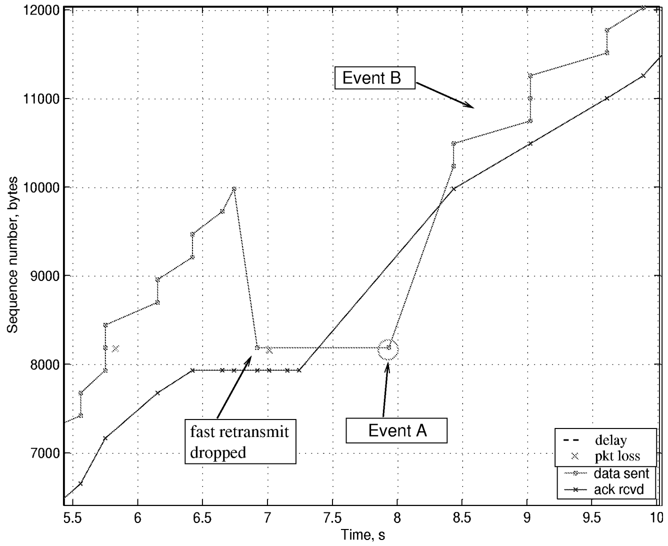


Figure 2: Sequence number vs. time in midst of some packet losses.

(a) (2 marks) What is the event A?

(b) (3 marks) Why did the ACK value jump from around 8000 to around 10000 at time 8.4s?

(c) (3 marks) What is the sender's `cwnd` value at time 9s, in terms of the number of `MSS`-sized packets, and why?

7. Consider the IP subnetted network in Fig. 3. The routers employ a routing protocol that does not carry subnet mask information (e.g., RIP-I). Therefore, the route's subnet mask is assumed to be the same as the subnet mask of the network interface where the route is received.

(a) (4 marks) Can a host on LAN D reach a host on LAN A and why?

(b) (4 marks) Consider a host on LAN C which configures $R1$ as its default router. The host sends packets to three destinations: `132.10.3.129`, `132.10.3.65`, and `132.10.2.1`. After sending the packets, what does the host's routing table look like? Note that ICMP redirect messages create host-specific routing entries.

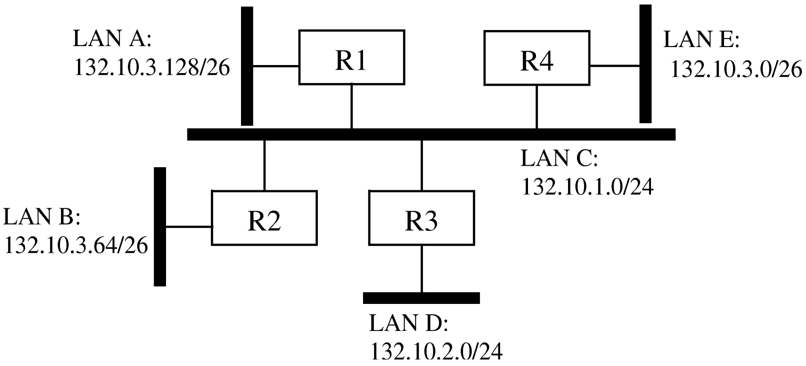


Figure 3: An IP network variable subnet masks.

8. Consider the OSPF network in Fig. 4. The costs of all the links (there are 20 of them) are set to 10 initially, and the link costs can be any positive integers. The routers B, C, D and E are meshed together to increase resilience against link and router failures.

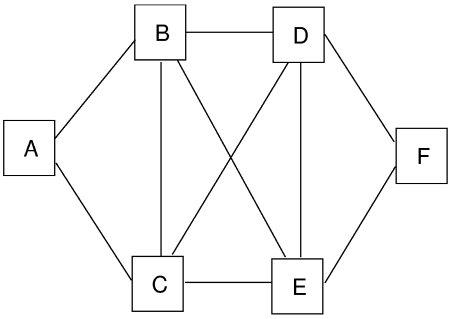


Figure 4: An OSPF network with 6 nodes.

(a) (2 marks) How many possible best paths for A to reach F, and what are they?

(b) (3 marks) Increase the link costs of at most 2 links just enough that the cross links $B-E$ and $C-D$ would not be used for A to reach F.

(c) (3 marks) Can F influence the best paths originated from A by changing the costs of its links? Explain your answer.

9. Fig. 5 shows an AS-level topology, and each link corresponds to a BGP connection as well as a forwarding path. The arrows represent BGP announcements of the prefixes in AS7. Each router chooses the best route based on the shortest AS path length which can be overridden by the `LOCAL-PREF` attribute. Moreover, AS3 always prefers the route announced from AS5 than from others for the same prefix, i.e., by choosing the appropriate `LOCAL-PREF` values.

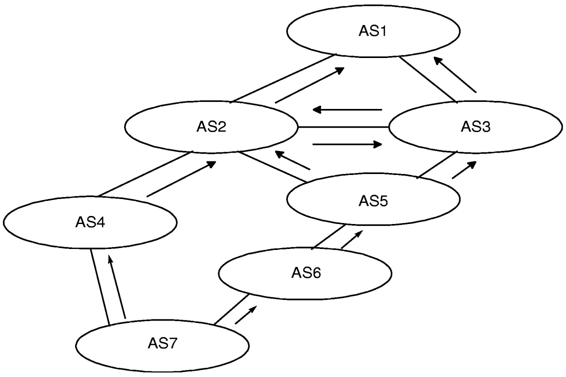


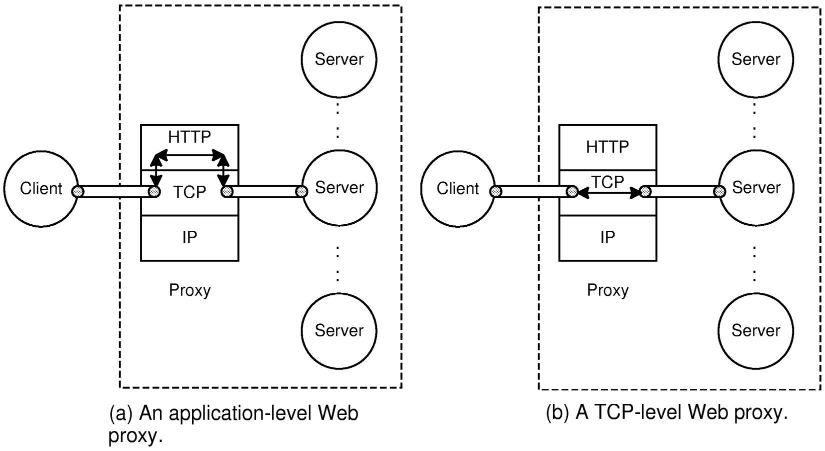
Figure 5: An AS topology.

(a) (4 marks) What would be the routing path for a packet originated from AS3 and destined for AS7? Explain your answer.

(b) (4 marks) What would be the routing path for a packet originated from AS1 and destined for AS7? Explain your answer.

Section B: Please answer both questions in this section.

10. (22 marks) In this question we consider a **TCP-level Web Proxy**. Fig. 6 shows that a Web proxy is situated between a client and a set of Web servers. The proxy terminates the TCP connection from the client, and sets up another TCP connection with a Web server. Here we are ignoring the proxy on the client's network. There are 2 possible mechanisms for the proxy to relay the request and data between the client and the server. The first one, which is the most common, shown in Fig. 6(a) in which the request and data will be relayed through the HTTP layer in the proxy. In the second approach, which is shown in Fig. 6(b), the relay is done only on the TCP layer. This question considers the second approach.



(a) An application-level Web proxy.

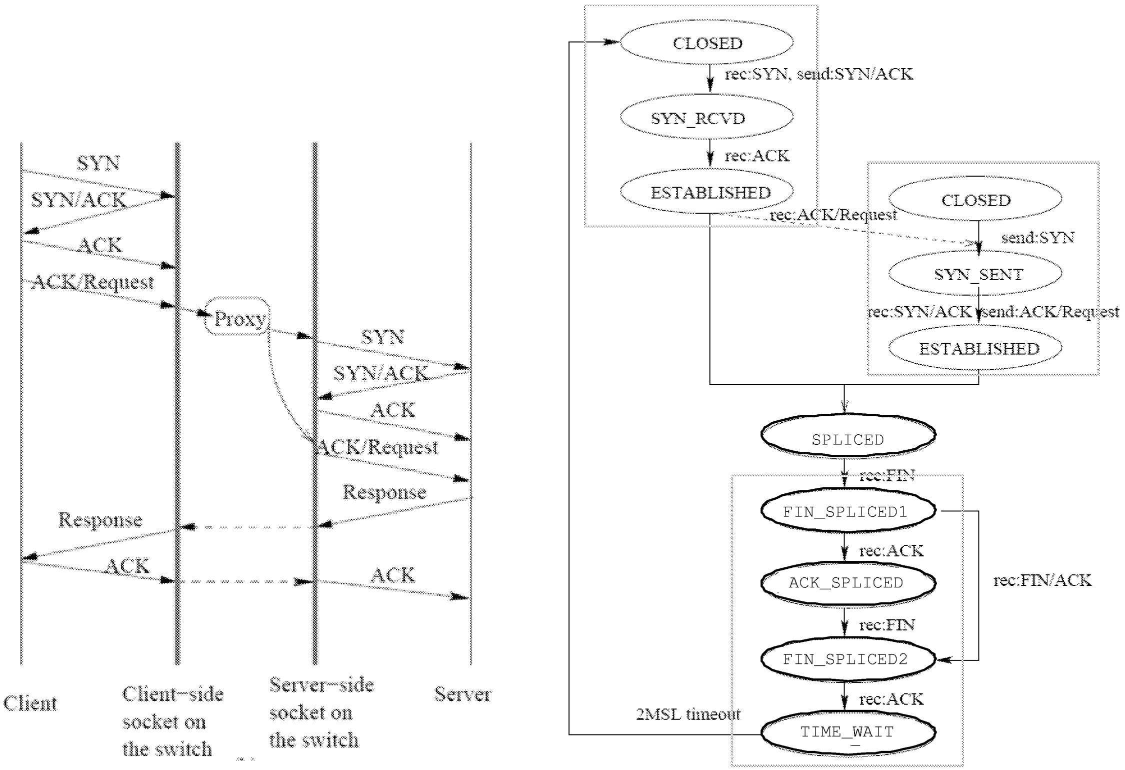
(b) A TCP-level Web proxy.

Figure 6: Application-level and TCP-level Web proxies.

To understand how the TCP-level Web proxy works, consider the packet exchange and state transition diagram in Fig. 7.

- When a client initiates a TCP `SYN` segment with a Web service's IP address and port, the proxy receives the `SYN` segment and performs a 3-way handshake with the client, i.e., establishing a TCP connection between the client and the proxy.
- After receiving the client's HTTP request, the proxy parses it and establishes another TCP connection with the appropriate server, also through a 3-way handshake, i.e., establishing a TCP connection between the proxy and the server.
- Then the proxy forwards the HTTP request to the server on the TCP layer.
- Upon receiving the response data from the server, the proxy forwards it to the client on the TCP layer.

- Note that the 2 TCP handshakings are the same for an application-level Web proxy and a TCP-level Web proxy. However, in - the subsequent data transmissions (TCP data and ACK), the TCP-level Web proxy simply forwards them on the TCP layer.



(a) Connection setup and the data transfer.

(b) State transition diagram.

Figure 7: Connection setup and the state transition diagram for a TCP-level Web proxy.

Let's consider the first TCP handshaking between the client and the proxy.

```
client                                                          Proxy
   ----> SYN, SN = CSEQ                                       ---->
   <---- SYN, SN = DSEQ, AN = CSEQ + 1                        <----
   ----> Data (HTTP request), SN = CSEQ + 1, AN = DSEQ + 1 ---->
```

After receiving the HTTP request which is of `lenR` bytes, the proxy creates a TCP connection to a server. In order to minimize changes in the subsequent forwarding to the server, the proxy uses the initial sequence number announced by the client. Therefore, the the handshaking messages are:

```
Proxy                                                        Server
   ----> SYN, SN = CSEQ                                       ---->
   <---- SYN, SN = SSEQ, AN = CSEQ + 1                        <----
   ----> Data (HTTP request), SN = CSEQ + 1, AN = SSEQ + 1    ---->
```

(a) (3 marks) After the second 3-way handshaking is completed. The proxy moves to the `SPLICED` state. The proxy first receives a TCP data segment from the server. Assume that the TCP data is of `lenD` bytes. What is the value of `AN` in this segment?

(b) (3 marks) Before forwarding the data segment received from the server to the client on the other TCP connection, the proxy needs to fill in the corresponding port numbers. Besides, it has to modify the `SN` value. What should the new value of `SN` be?

(c) (3 marks) Assume that the client has received the first data segment and it returns a pure ACK. Similarly, the proxy receives the ACK and forward it to the server. In this case, the proxy needs to modify the value of `AN` before forwarding. What is the value of `AN` sent by the client to proxy, and what is the modified value of `AN` sent by the proxy to the server?

(d) (3 marks) In general, the forwarding of data from the server to the client requires a modification of the `SN`. If the `SN` in the data sent from the server is given by `SN_NO`, what would be the value of the modified `SN` in the data sent from the proxy to the client?

(e) (3 marks) In general, the forwarding of ACKs from the client to the server requires a modification of the `AN`. If the `AN` sent from the client is given by `ACK_NO`, what would be the value of the modified `AN` in the segment sent from the proxy to the server?

(f) (5 marks) Now let's consider the connection termination phase, starting from the state `FIN_SPLICED1`. The state transitions in the connection termination in Fig. 7(b) are the same whether the server or the client initiates the `close()`. Draw a timeline diagram, similar to the one on p. 20 of the *TCP and UDP Basics* slides, for the case where the client initiates the close. You do not have to show the `SN` and `AN`.

(g) (2 marks) Why does the client *always* arrive at the `TIME_WAIT` state which is not always the case for a typical TCP connection?

11. (22 marks) Consider the IP network in Fig. 8 which is the same as the one in assignment 3. The routers are running RIP with split horizon with poisonous reverse among themselves. In this question, we consider how a host broadcasts a packet to all subnets in the network. The destination address is therefore a network-directed address and all routers are configured to forward such broadcast packets.

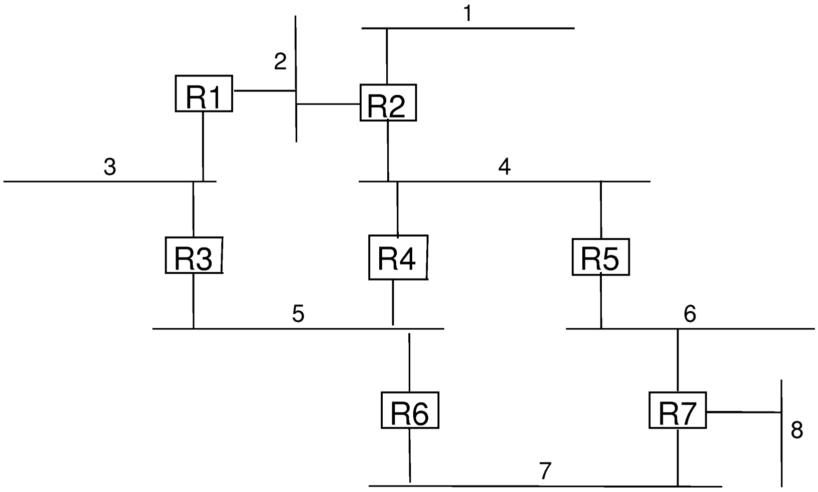


Figure 8: An IP network topology.

Now consider the following method that is used by the routers to broadcast packets. Let the source address in the broadcast packet be S. Consider a router *R* that receives the broadcast packet from interface I.

```
From the forwarding table, R first determines that it would send out
a packet destined to S to interface SI.
If (SI not equal to I)
   Discard the broadcast packet.
else
   Receive the broadcast packet and send a copy to other interfaces.
```

We refer the interface SI that receives the broadcast packets sent by S as the *receiving interface*, and other interfaces as *nonreceiving interfaces*. The following questions help you understand how this broadcast mechanism works. For this purpose, consider that a host on subnet 5 broadcasts a packet.

(a) (3 marks) Indicate in the following table the receiving interfaces for the broadcast packet. E, S, W, and N represent the East, South, West, and North interfaces, respectively.

	E	S	W	N
$R1$			NA	NA
$R2$	NA			
$R3$	NA		NA	
$R4$	NA		NA	
$R5$	NA		NA	
$R6$	NA		NA	
$R7$			NA	

(b) (3 marks) For each subnet, except 5, which router(s) is responsible for delivering the broadcast packet to that subnet?

Subnet	Router(s)
1	
2	
3	
4	
5	NA
6	
7	
8	

(c) (3 marks) Which subnet(s), except 5, does *not* have the hop count of 16 for reaching subnet 5 in the RIP messages and why?

(d) (2 marks) Would the broadcast mechanism create routing loops? Explain your answer.

(e) (3 marks) Under what condition would a subnet receive duplicate broadcast packets?

(f) (4 marks) In fact, a router is able to determine from the RIP messages whether duplicate broadcast packets would be sent on the subnet. Explain how the router can determine it.

(g) (4 marks) Propose an enhancement to the algorithm above that would eliminate the problem of duplicate broadcast packet.

— End of the Examination Paper —