THE HONG KONG POLYTECHNIC UNIVERSITY

Department of Computing

This is an open-book examination.

(COMP5311)

Internet Infrastructure and Protocols

22 December 2008 3.5 hours

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

Section A: Please answer AT MOST SEVEN questions in this section [8 marks each, making up a total of 56 marks out of 100]. You should always attach a succinct explanation to your answer.

---

1. (IP broadcast + variable-length subnet mask) Consider the network segment in Figure 1. The four hosts, though belonging to the same class B network, are configured with different subnet masks. Answer the following questions with explanations. Assume that all-subnets-directed-broadcast is supported, and all subnet and host bits are set to 1 for this address.

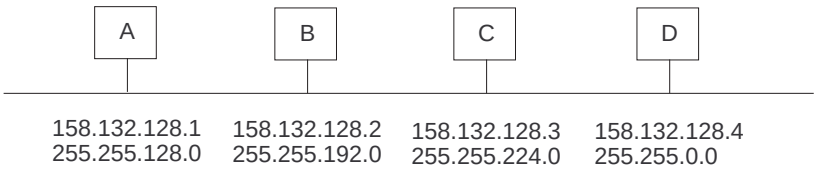


Figure 1: A network of four IP hosts.

   (a) (3 marks) If host A sends a broadcast IP packet for its own subnet (i.e., destination address is `158.132.255.255`), will other hosts receive this broadcast packet?

   (b) (3 marks) If host B sends a broadcast IP packet for its own subnet, will other hosts receive this broadcast packet?

   (c) (2 marks) If host C sends a broadcast IP packet for its own subnet, will other hosts receive this broadcast packet?

2. (IP tunnel and fragmentation) Consider that an IP packet of 1500 bytes entering into a router R and the packet will be tunneled before forwarding. The DF (don't fragment) bit in the IP packet is on. The router's incoming and outgoing links have the MTU of 1500 bytes. Therefore, IP fragmentation is required for this packet. Moreover, the DF bit of the tunnel header is always off. Answer the following questions.

   (a) (4 marks) Assume that the IP fragmentation is performed based on tunneling-then-fragmentation. How did R process the IP packet? If the packet will be forwarded, describe the details about forwarded fragments, such as the size. If the packet is not forwarded, describe R's other possible actions.

   (b) (4 marks) Repeat part (a) for fragmentation-then-tunneling.

3. (Proxy ARP) Referring to Figure 2, host H performs proxy ARP for three subnets. For the following cases, H will reply the ARP request on behalf of the target host. What is the target MAC address returned in the ARP reply? You may refer the routers' two interfaces to as upper and lower.

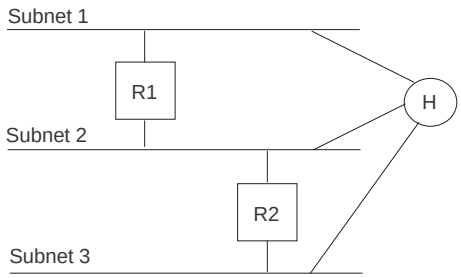


Figure 2: Host H performs proxy ARP for subnets 1, 2, and 3.

   (a) (2 marks) In the ARP request message, the source IP address belongs to subnet 1 and the target IP address belongs to a different subnet.
   (b) (2 marks) In the ARP request message, the source IP address belongs to subnet 3 and the target IP address belongs to a different subnet.
   (c) (2 marks) In the ARP request message, the source IP address belongs to subnet 2 and the target IP address belongs to subnet 1.
   (d) (2 marks) In the ARP request message, the source IP address belongs to subnet 2 and the target IP address belongs to subnet 3.

4. (ICMP redirect) As depicted in Figure 3, $R2$ may receive packets from either a router ($R1$) or a host (H). However, $R2$ only uses ICMP redirect to inform a host for a better route, for example, via $R3$ on the same subnet. $R2$ will not use ICMP redirect for routers, because the routing protocol can already handle it.

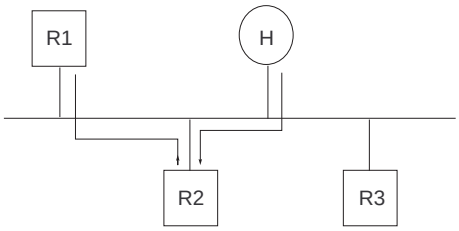


Figure 3: $R2$ could receive a packet from a host or a router.

   Therefore, after forwarding a packet and detecting a triangular route, $R2$ has to decide whether it should send an ICMP redirect. How does $R2$ make that decision?

5. (TCP transmissions) Consider the following tcpdump traces for a TCP data connection. The sender's MSS is 512 bytes. On line 1, host A sent 512 bytes of data to host B at time `12:00:48.442538`. In this data packet, the TCP sequence number is 995409 and the ACK number is 1. On the second line, an ACK packet was sent from B, and the advertised window size was 4096 bytes.

```
12:00:48.442538 A > B: . 995409:995921(512) ack 1
12:00:48.544483 B > A: . ack 991825 win 4096
12:00:49.044613 A > B: . 991825:992337(512) ack 1
12:00:49.192282 B > A: . ack 995921 win 2048
12:00:49.193392 A > B: . 995921:996433(512) ack 1
12:00:49.194726 A > B: . 996433:996945(512) ack 1
12:00:49.350665 B > A: . ack 996945 win 4096
12:00:49.351694 A > B: . 996945:997457(512) ack 1
12:00:49.352168 A > B: . 997457:997969(512) ack 1
12:00:49.352643 A > B: . 997969:998481(512) ack 1
```

   Answer the following questions:

   (a) (2 marks) Describe the event on the third line.

   (b) (2 marks) Describe the event on the fourth line.

   (c) (2 marks) What is the maximum number of bytes that A can send after receiving the ACK on the fourth line and explain why?

   (d) (2 marks) Explain why A could send three consecutive MSS-sized segments on the last three lines?

6. (TCP's fast retransmission and fast recover) Consider the following tcpdump traces for a TCP data connection. The sender's MSS is 512 bytes. At `10:10:56.825635`, the sender's `cwnd` is seven segments.

```
10:10:56.825635 A > B: . 229697:230209(512) ack 1
10:10:57.038794 B > A: . ack 227649 win 4096
10:10:57.039279 A > B: . 230209:230721(512) ack 1
10:10:57.321876 B > A: . ack 228161 win 4096
10:10:57.322356 A > B: . 230721:231233(512) ack 1
10:10:57.347128 B > A: . ack 228673 win 4096
10:10:57.347572 A > B: . 231233:231745(512) ack 1
10:10:57.347782 A > B: . 231745:232257(512) ack 1
10:10:57.936393 B > A: . ack 229185 win 4096
10:10:57.936864 A > B: . 232257:232769(512) ack 1
10:10:57.950802 B > A: . ack 229697 win 4096
10:10:57.951246 A > B: . 232769:233281(512) ack 1
10:10:58.169422 B > A: . ack 229697 win 4096
10:10:58.638222 B > A: . ack 229697 win 4096
10:10:58.643312 B > A: . ack 229697 win 4096
10:10:58.643669 A > B: . 229697:230209(512) ack 1
```

```
10:10:58.936436 B > A: . ack 229697 win 4096
10:10:59.002614 B > A: . ack 229697 win 4096
10:10:59.003026 A > B: . 233281:233793(512) ack 1
10:10:59.682902 B > A: . ack 233281 win 4096
10:10:59.683391 A > B: . 233793:234305(512) ack 1
10:10:59.683748 A > B: . 234305:234817(512) ack 1
```

(a) (1 mark) What is the event occurred at `10:10:58.643669`?

(b) (3 mark) What is A's `cwnd` at `10:10:58.643669`?

(c) (1 mark) What is A's `cwnd` at `10:10:58.936436`?

(d) (2 marks) Why could A send a new data segment at `10:10:59.003026`?

(e) (1 mark) What is A's `cwnd` at `10:10:59.682902`?

7. (RIP with split horizon) In Figure 4, two RIP routers $R1$ and $R2$ are exchanging routes for destination D. Assume that they are using split horizon with poisonous reverse. In the case of equal-cost path, a router just selects any of them.

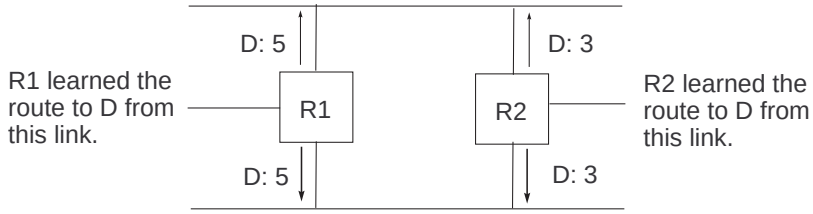


Figure 4: Two RIP routers $R1$ and $R2$ are exchanging routes for destination D.

(a) (2 marks) Assume that there are no changes in the distance vectors concerning D. In the steady state, what are the distance vectors announced on the two subnets.

(b) (6 marks) Now $R2$'s right line to D is no longer available. Assume that $R2$ does not announce the updated distance (i.e., 16) to D. $R2$ will also accept a better route immediately. Explain in detail steps whether there will be a permanent routing loop between $R1$ and $R2$.

8. (RIP with path inflation) A RIP router initially advertises its presence with a distance of 0. Now consider a special RIP router $R1$ that has two links. $R1$ advertises a distance of 0 to link 1 and a distance of $n > 0$ to link 2. Note that for some reasons $R1$ artificially inflates the length of the route advertised to link 2. Assume that the network is connected. Discuss the possible effect of the path inflation on the forwarding path from another router $R2$ to $R1$ for the following scenarios. Explain your answers clearly.

(a) (2 marks) If no path inflation is introduced, $R2$'s packets can be received by $R1$ via either link, because the two paths are equally good.

(b) (3 marks) If no path inflation is introduced, $R2$'s packets will be received by $R1$ via link 1. Assume that there are no equal-cost paths.

(c) (3 marks) If no path inflation is introduced, $R2$'s packets will be received by $R1$ via link 2. Assume that there are no equal-cost paths.

9. (Link-state routing) In a link-state routing protocol, a link failure has to be broadcasted to all other routers to update their link-state databases. A COMP5311 student, however, claims that it is not necessary to disseminate the link failure update to all routers. Instead, only the routers on the *restoration path* need to be updated. Figure 5 illustrates this student's idea. The link between $R1$ and $R2$ fails, and the restoration path for $R1 - R2$ is through $R4$. Therefore, only $R1$, $R2$, and $R4$ will update the link states for $R1 - R2$ to "unreachable". $R3$ and $R5$, on the other hand, are not aware of the link failure.

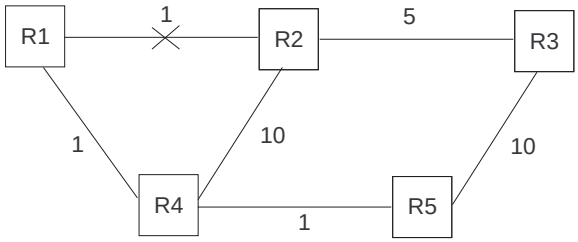


Figure 5: A network running a link-state routing protocol.

(a) (4 marks) Use a simple example to illustrate that this scheme will result in a routing loop.

(b) (4 marks) Use a simple example to illustrate that this scheme will result in a nonshortest path.

10. (OSPF) Referring to the OSPF network below, answer the following questions:

(a) (1 mark) Is $RT1$ aware of $RT4$ and why?

(b) (1 mark) Is $RT1$ aware of $RT5$ and why?

(c) (1 mark) Is $RT1$ aware of $RT6$ and why?

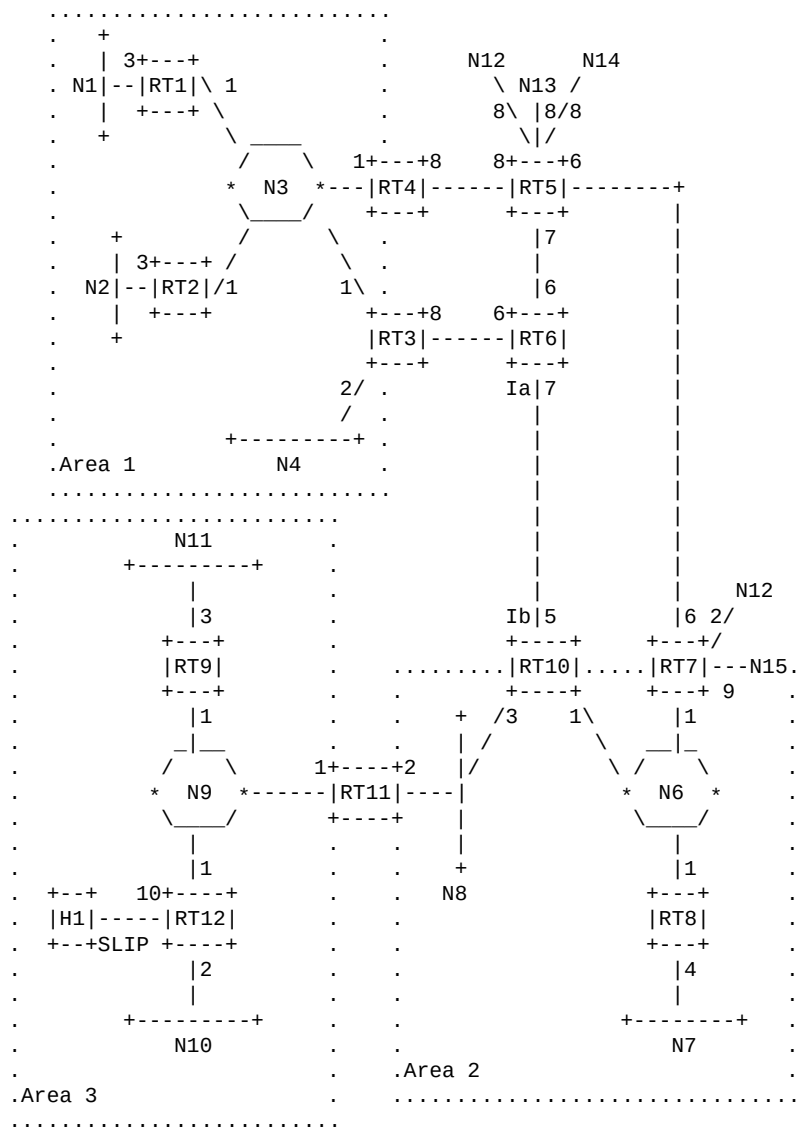
(d) (1 mark) Is $RT1$ aware of $RT7$ and why?

(e) (1 mark) Is $RT1$ aware of $RT8$ and why?

(f) (1 mark) Is $RT3$ aware of $RT5$ and why?

(g) (1 mark) Is $RT3$ aware of $RT8$ and why?

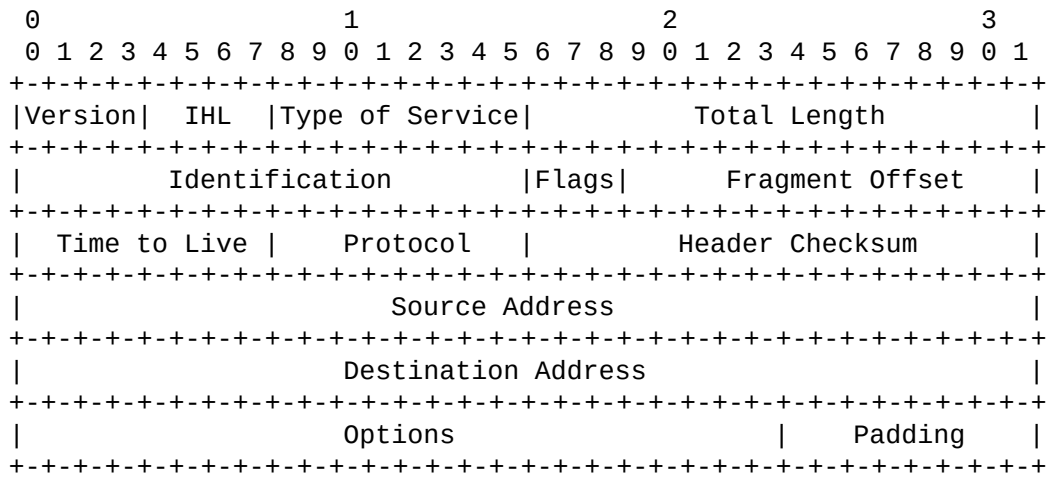
(h) (1 mark) Is $RT3$ aware of $RT11$ and why?


N12
N14
N13
N1
RT1
N3
RT4
RT5
N2
RT2
RT3
RT6
N4
Area 1
N11
RT9
N12
RT10
RT7
N15
N9
RT11
N6
H1
RT12
SLIP
N8
RT8
N10
N7
Area 2
Area 3

Section B: Please answer both questions in this section. Each question carries 22 marks.

---

11. (Miscellaneous questions about IP) This question concerns various aspects about IP, including packet processing, fragmentation, and option processing.



(a) (4 marks) When a router receives an IP packet in an IP version 4 network, it should drop it for the following cases. Fill in the missing values and offer brief explanations for your answers:

- IP version is not equal to 4.
- The header length is less than _____ bytes or greater than _____ bytes.
- The total length exceeds _____ bytes.
- TTL is equal to _____.
- Checksum is incorrect.

(b) (2 mark) Why is the fragment offset in the unit of 8 bytes?

(c) (2 marks) Compare the header of an IP packet and the header of its fragments. Which of the following fields will **definitely** be different? Explain your answers.

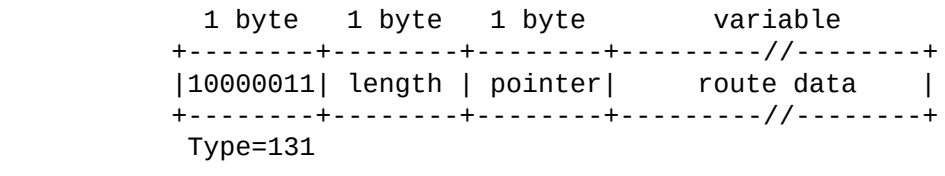
- The total length
- The IPID
- The fragment offset
- The `M` bit

(d) (2 marks) A COMP5311 student proposed that a retransmitted IP packet should use the same IPID (the identification field in IP) for the original packet. Suggest one possible advantage of this proposal.

(e) (2 marks) IPv6 supports only end-to-end packet fragmentation. That is, only the sender is allowed to fragment an IP packet. Are the three IPv4 fragmentation and reassembly mechanisms—IPID, fragment offset, and `M` bit—still needed for IPv6 fragmentation and reassembly?

(f) (2 marks) When a router receives an IP packet, it has to determine whether it has one or more IP options, because the ones with options will be processed on a different path. How can the router determine that?

(g) (2 marks) The format of the loose source route (LSR) option is given by



The route data consist of a series of IP addresses, each of which takes up 4 bytes. What is the maximum number of IP addresses that can be supported if there are no other IP options?

(h) (2 marks) How does an IP node determine whether it is the destination of an IP datagram with the LSR option?

(i) (2 marks) If an IP packet containing a LSR option is fragmented, will each fragment contain the option and why?

(j) (2 marks) ICMP redirect will be suppressed for IP packets with the LSR option. Why?

12. (Designing a port scanning method) The purpose of this question is to design a port scanning method. An attacker Alice wants to know the TCP ports of Vicky (the victim) that are running applications. Moreover, to prevent her identity to be discovered, Alice will spoof to be Peter in the scanning process. Peter must be running an operating systems that increment the IPID (the identification field in the IP header) by one for every packet sent, regardless of its destination.

    The following facts will be useful for this question:

    - A TCP SYN segment arriving for a closed port will be dropped. Moreover, it triggers an RST segment sent back to the sender.
    - A TCP ACK packet arriving for a closed port will be dropped. Moreover, it triggers an RST segment sent back to the sender.
    - An RST segment arriving for a listening or closed port will be dropped silently.

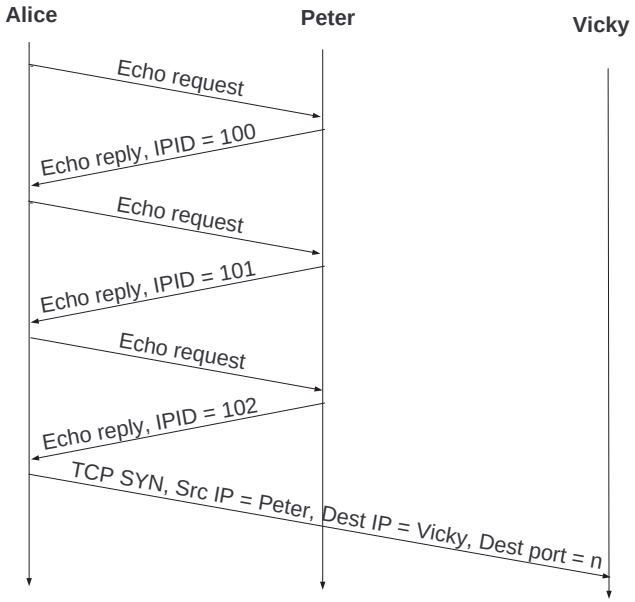


Figure 6: The first two steps of the port scanning attack launched by Alice.

(a) (2 marks) The first step of the attack is for Alice to send a number of ICMP echo requests (i.e., ping) to Peter which responds with ICMP echo replies. After that, Alice sends a TCP SYN segment to Vicky on port n, and the packet's source IP address is Peter's. Figure 6 illustrates the first two steps. Assume that there is no TCP service running at port n for this part and (b)-(c). How will Vicky respond to this TCP SYN packet?

(b) (2 marks) After the first two steps, Alice continues to send a few more (say three more) ICMP echo request packets to Peter and receives the corresponding ICMP echo reply packets from Peter. What are the IPIDs in the ICMP echo reply packets? You may assume that no one else is using Peter to send packets.

(c) (3 marks) How does Alice detect from the above that port n at Vicky is closed?

(d) (3 marks) Repeat part (a) for the case that a TCP service is running at port n.

(e) (3 marks) Repeat part (b) for the case that a TCP service is running at port n.

(f) (3 marks) How does Alice detect from the above that port n at Vicky is open?

(g) (3 marks) One solution to mitigating the attack is to put an intrusion prevention box (IPS) in front of Peter. The IPS will scramble the IPIDs of the incoming and outgoing packets. That is, each IPID is modified to a different value. Discuss how the IPS will affect ICMP error messages sent out from Peter?

(h) (3 marks) Another solution is to put an IPS in front of Vicky. This IPS will send a TCP ACK packet immediately after every RST packet sent out from Vicky. The TCP ACK packet and RST packet have the same source and destination socket addresses. Explain how this IPS foils the port scanning attack.

— End of the Examination Paper —