Internet Infrastructure and Protocols (COMP5311)

Assignment One (due on 19 Oct 2011)
Each question carries 8 marks, unless stated otherwise.

Rocky K. C. Chang

1) A certain class B network `160.10.0.0/16` is subnetted according to the following structure. Note that variable length subnet mask is used and the subnetting is done with a certain pattern.

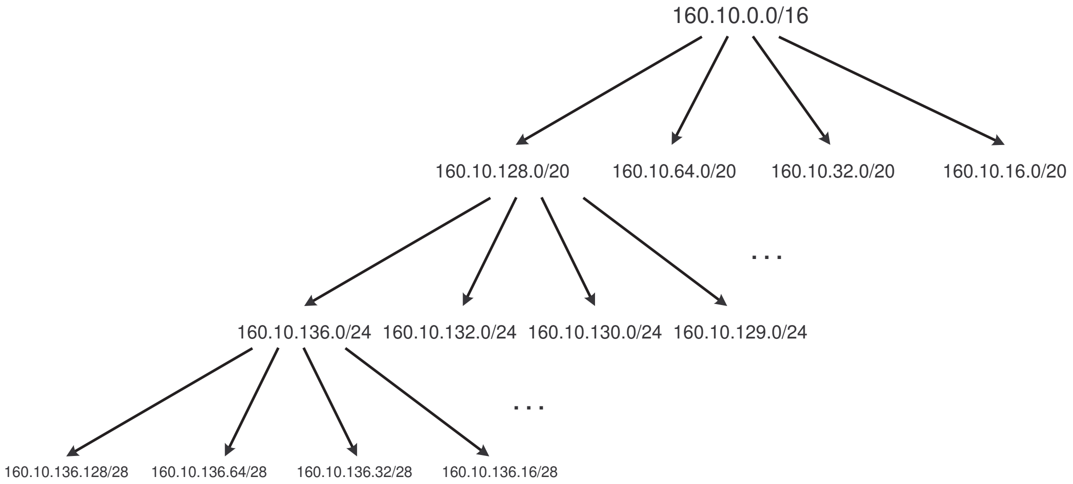

Fig. 1. The subnet structure of `160.10.0.0/16`.

a) (3 marks) Which subnet corresponds to the subnet-directed broadcast address `160.10.47.255`?
b) (3 marks) Which subnet corresponds to the subnet-directed broadcast address `160.10.130.31`?
c) (2 marks) Is `160.10.127.255` a subnet-directed broadcast address in this class B network?

2) Consider that an IP packet of 1500 bytes (with destination address as D and a 20-byte IP header) entering into a router R, and the packet will be tunneled before forwarding. The tunnel MTU is assumed to be 1480 bytes. Therefore, IP fragmentation is required for this packet. In this question, we explore a fragment-first-and-then-tunnel approach. Using this approach, the IP packet will be first fragmented in packets not exceeding the tunnel MTU, and then each fragment is tunneled by encapsulating the fragment with a 20-byte IP header.

a) (3 marks) What is the size of the second fragment?
b) (3 marks) If there is no further fragmentation, where will the fragments be reassembled? The exit tunnel endpoint or D?

c) (2 marks) If the fragments are further fragmented in the path between the two tunnel endpoints, where will these fragments of fragments be reassembled? Assume that there is no other IP tunnel in the path.

3) In a ping of death attack, an attacker sends out an IP datagram that exceeds the maximum size of an IP datagram (65,535 bytes). Since this attack packet will be fragmented, the victim would not know the actual size of the original packet until it attempts to reassemble the fragments. However, some systems do not know how to handle an IP datagram of more than the maximum size; as a result, the attack causes them to hang and to reboot.

   The following is a tcpdump trace of such an attack. The fragmentation is performed according to an MTU of 1500 bytes, and the IP headers do not contain options.

```
17:26:11.013622 cslwin95 > arkroyal: icmp: echo request (frag 6144:1480@0+)
17:26:11.015079 cslwin95 > arkroyal: (frag 6144:1480@1480+)
17:26:11.016637 cslwin95 > arkroyal: (frag 6144:1480@2960+)
17:26:11.017577 cslwin95 > arkroyal: (frag 6144:1480@4440+)
17:26:11.018833 cslwin95 > arkroyal: (frag 6144:1480@5920+)
17:26:11.020112 cslwin95 > arkroyal: (frag 6144:1480@7400+)
17:26:11.021346 cslwin95 > arkroyal: (frag 6144:1480@8880+)
17:26:11.022641 cslwin95 > arkroyal: (frag 6144:1480@10360+)
17:26:11.023869 cslwin95 > arkroyal: (frag 6144:1480@11840+)
17:26:11.025140 cslwin95 > arkroyal: (frag 6144:1480@13320+)
17:26:11.026604 cslwin95 > arkroyal: (frag 6144:1480@14800+)
17:26:11.027628 cslwin95 > arkroyal: (frag 6144:1480@16280+)
17:26:11.028871 cslwin95 > arkroyal: (frag 6144:1480@17760+)
17:26:11.030100 cslwin95 > arkroyal: (frag 6144:1480@19240+)
17:26:11.031307 cslwin95 > arkroyal: (frag 6144:1480@20720+)
17:26:11.032542 cslwin95 > arkroyal: (frag 6144:1480@22200+)
17:26:11.033774 cslwin95 > arkroyal: (frag 6144:1480@23680+)
17:26:11.035018 cslwin95 > arkroyal: (frag 6144:1480@25160+)
17:26:11.036576 cslwin95 > arkroyal: (frag 6144:1480@26640+)
17:26:11.037464 cslwin95 > arkroyal: (frag 6144:1480@28120+)
17:26:11.038696 cslwin95 > arkroyal: (frag 6144:1480@29600+)
17:26:11.039966 cslwin95 > arkroyal: (frag 6144:1480@31080+)
17:26:11.041218 cslwin95 > arkroyal: (frag 6144:1480@32560+)
17:26:11.042579 cslwin95 > arkroyal: (frag 6144:1480@34040+)
17:26:11.043807 cslwin95 > arkroyal: (frag 6144:1480@35520+)
17:26:11.046276 cslwin95 > arkroyal: (frag 6144:1480@37000+)
17:26:11.047236 cslwin95 > arkroyal: (frag 6144:1480@38480+)
17:26:11.048478 cslwin95 > arkroyal: (frag 6144:1480@39960+)
17:26:11.049698 cslwin95 > arkroyal: (frag 6144:1480@41440+)
17:26:11.050929 cslwin95 > arkroyal: (frag 6144:1480@42920+)
17:26:11.052164 cslwin95 > arkroyal: (frag 6144:1480@44400+)
17:26:11.053398 cslwin95 > arkroyal: (frag 6144:1480@45880+)
17:26:11.054685 cslwin95 > arkroyal: (frag 6144:1480@47360+)
17:26:11.056347 cslwin95 > arkroyal: (frag 6144:1480@48840+)
17:26:11.057313 cslwin95 > arkroyal: (frag 6144:1480@50320+)
17:26:11.058357 cslwin95 > arkroyal: (frag 6144:1480@51800+)
17:26:11.059588 cslwin95 > arkroyal: (frag 6144:1480@53280+)
17:26:11.060787 cslwin95 > arkroyal: (frag 6144:1480@54760+)
17:26:11.062023 cslwin95 > arkroyal: (frag 6144:1480@56240+)
17:26:11.063247 cslwin95 > arkroyal: (frag 6144:1480@57720+)
17:26:11.064479 cslwin95 > arkroyal: (frag 6144:1480@59200+)
17:26:11.066252 cslwin95 > arkroyal: (frag 6144:1480@60680+)
17:26:11.066957 cslwin95 > arkroyal: (frag 6144:1480@62160+)
17:26:11.068220 cslwin95 > arkroyal: (frag 6144:1480@63640+)
17:26:11.069107 cslwin95 > arkroyal: (frag 6144:398@65120)
```

Answer the following questions concerning the trace.

a) (1 mark) What does the number immediately before ”@” represent?
b) (1 mark) What does the number immediately after ”@” represent?
c) (1 mark) What does the ”+” symbol represent?
d) (1 mark) What is the number 6144 referred to?
e) (4 marks) What is the size of the original IP packet before fragmentation?

4) Consider a class B network `158.132.0.0` which is subnetted with a subnet mask of `255.255.255.0`. Moreover, a host with IP address `158.132.1.1` is compromised in that an attack program was installed in that machine. Discuss the effect of the attack if the attack program in that machine sends out an ICMP echo request message (ping) with the following source and destination addresses. Note that the source addresses in ping messages are spoofed (i.e., not equal to `158.132.1.1`). Assume the followings:

- All routers inside the network turn off the support for subnet-directed and all-subnet-directed IP broadcasts, i.e., drop those packets.
- All nodes (hosts and routers) must reply with an ICMP echo reply message when receiving an ICMP echo request message.
- When forwarding a packet, a router only examines the destination IP address, but not the source IP address.
- The destination addresses of the ping messages belong to hosts, but not to routers.

a) (3 marks) Source address = `158.132.1.100` and destination address = `255.255.255.255`.
b) (3 marks) Source address = `158.132.2.100` and destination address = `255.255.255.255`.
c) (2 marks) Source address = `158.132.2.100` and destination address = `158.132.2.255`.

5) An IP packet with a total length of 3000 bytes and a header length of 20 bytes is to be fragmented into 1500-byte IP packets.

a) (3 marks) Write down total length, the offset values, and the M-bit value in each fragment.
b) (2 marks) If the total length is changed to 3100 bytes, how would your answers be different from (a)?
c) (3 marks) If the header length becomes 40 bytes (and the IP packet’s total length remains 3000 bytes), how would your answers be different from (a)?